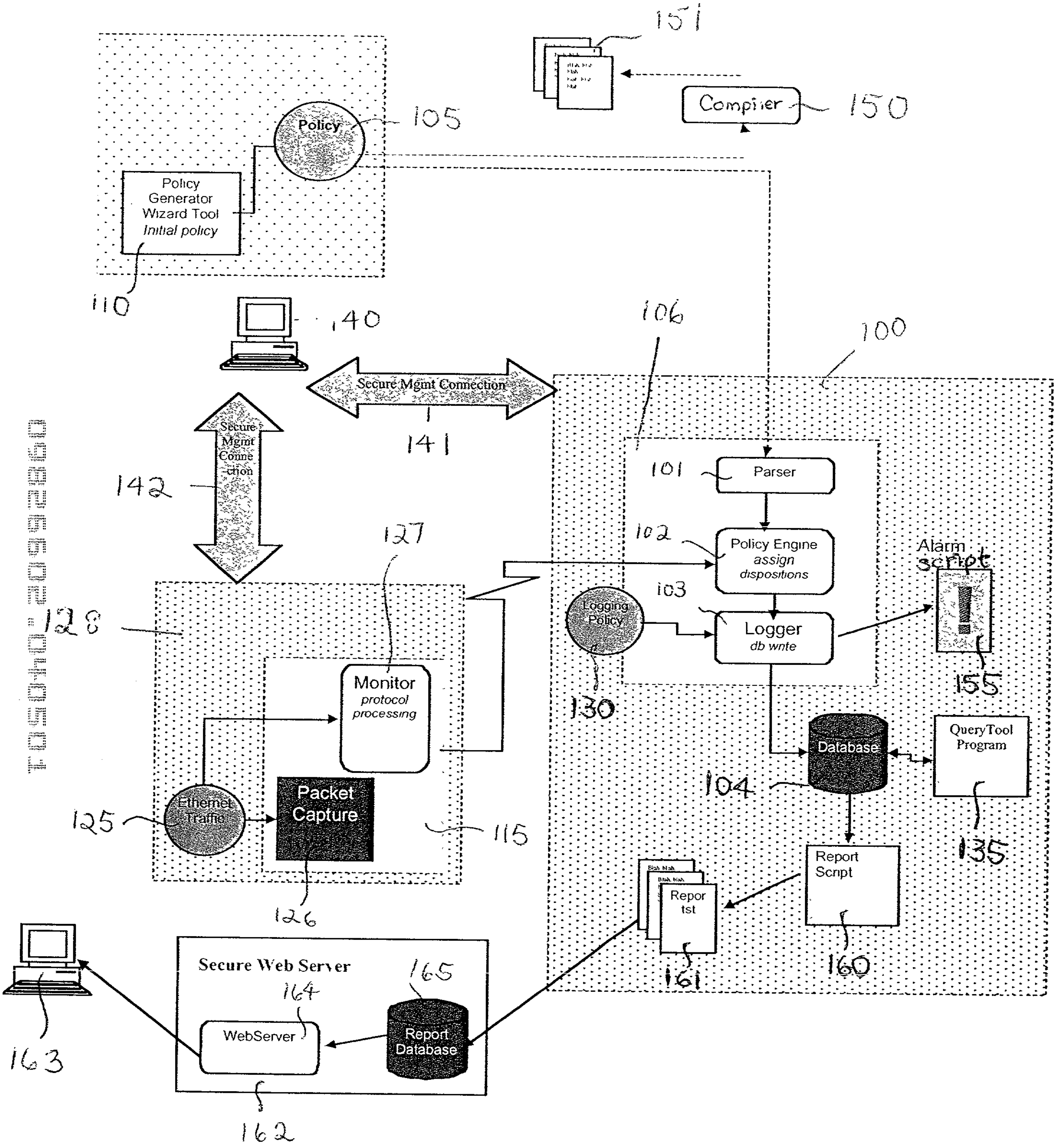

151
Compiler
150
Policy
105
Policy Generator Wizard Tool
Initial policy
110
140
106
100
Secure Mgmt Connection
141
Secure Mgmt Connection
142
101
Parser
102
Policy Engine
assign dispositions
Alarm script
103
Logging Policy
Logger
db write
155
130
127
128
Monitor
protocol processing
Ethernet Traffic
Packet Capture
125
115
126
Database
QueryTool Program
104
135
Report Script
Report tst
160
161
Secure Web Server
165
164
WebServer
Report Database
163
162

Figure 1a

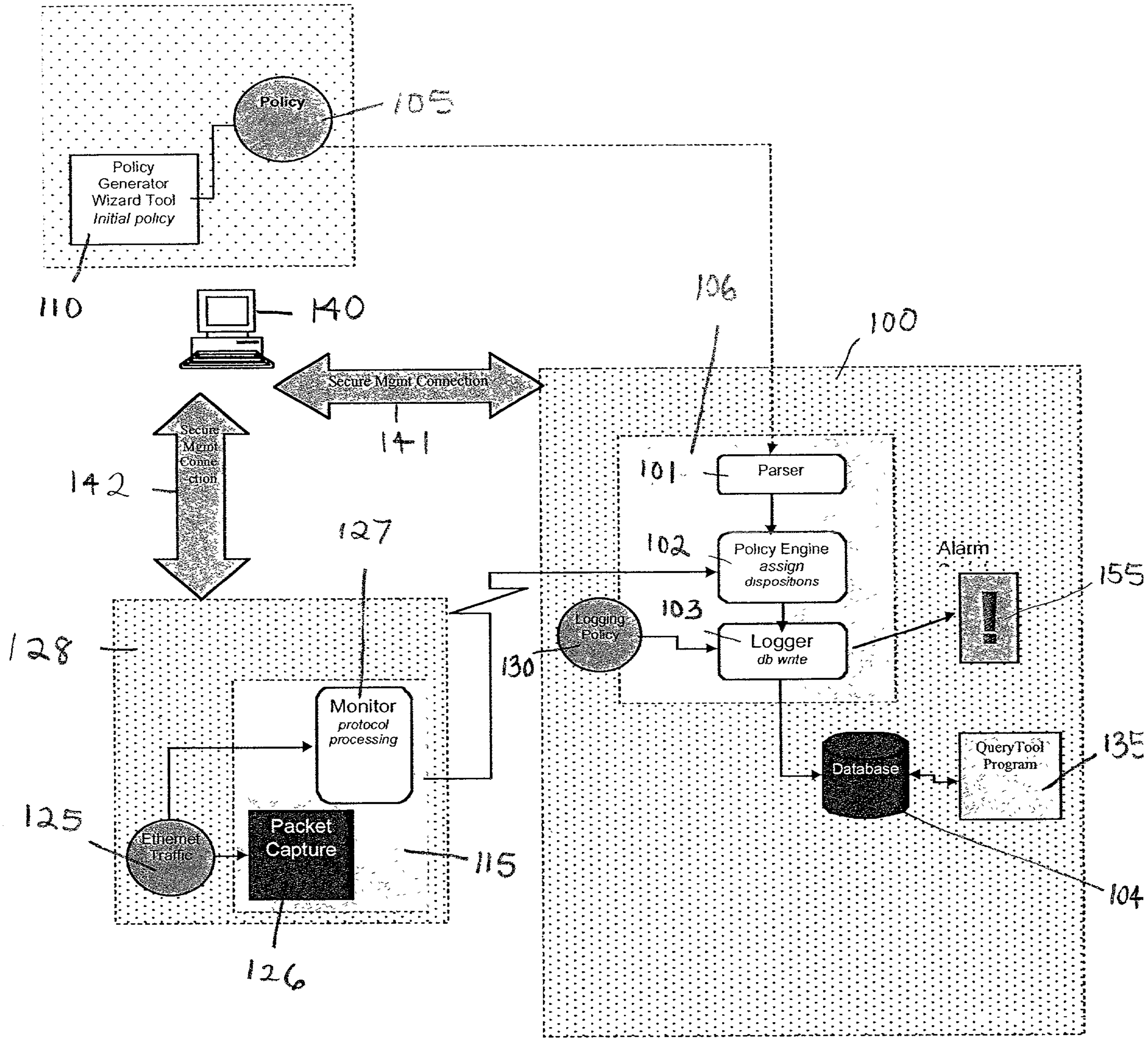

Policy
105
Policy Generator Wizard Tool *Initial policy*
110
140
106
100
Secure Mgmt Connection
141
Secure Mgmt Connection
142
101
Parser
127
102
Policy Engine *assign dispositions*
Alarm
155
103
Logging Policy
Logger *db write*
128
130
Monitor *protocol processing*
Database
QueryTool Program
135
125
Ethernet Traffic
Packet Capture
115
104
126

Figure 1b

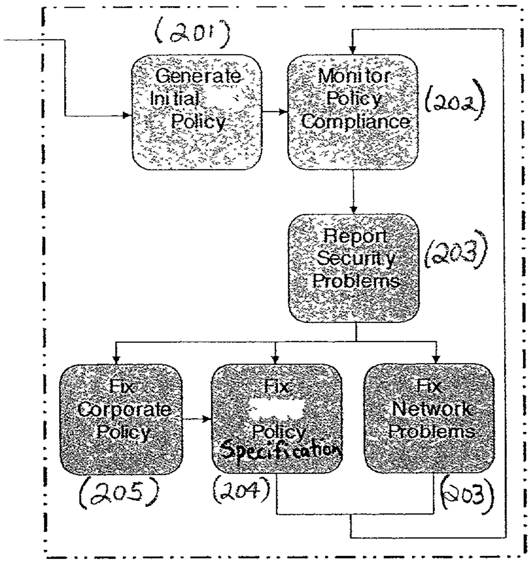
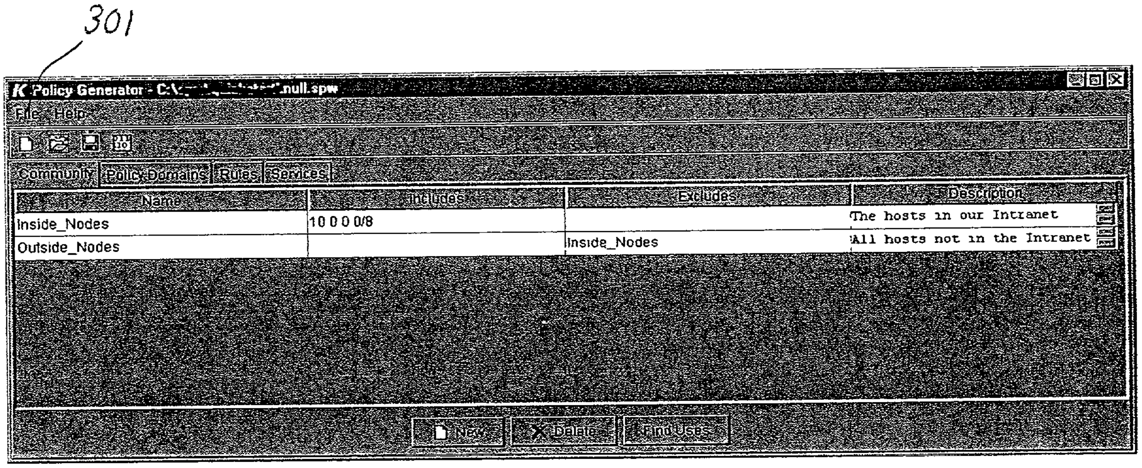

(201)
Generate Initial Policy
Monitor Policy Compliance
(202)
Report Security Problems
(203)
Fix Corporate Policy
Fix Policy Specification
Fix Network Problems
(205)
(204)
(203)

Fig. 2

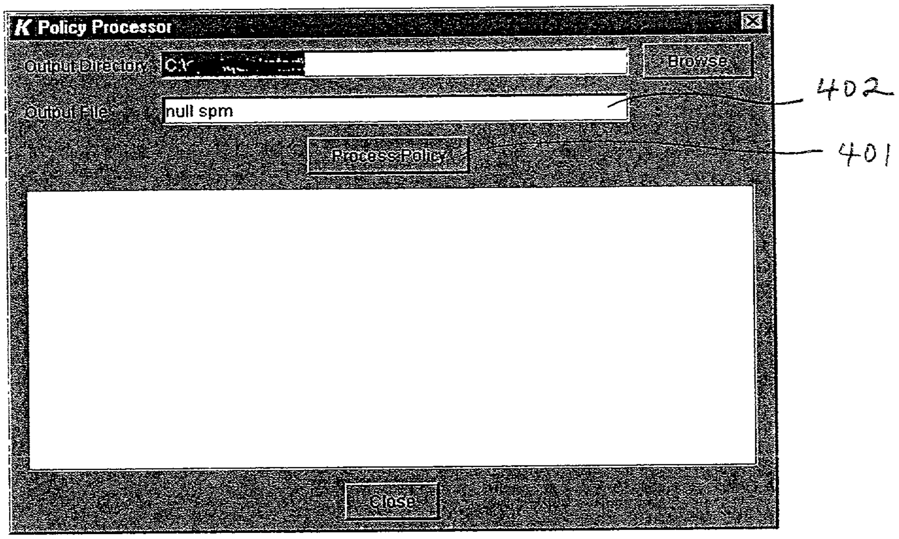
Fig. 3



Policy Generator - C:\[illegible]null.spw

Name	Includes	Excludes	Description
Inside_Nodes	10 0 0 0/8		The hosts in our Intranet
Outside_Nodes		Inside_Nodes	All hosts not in the Intranet

Fig. 4a

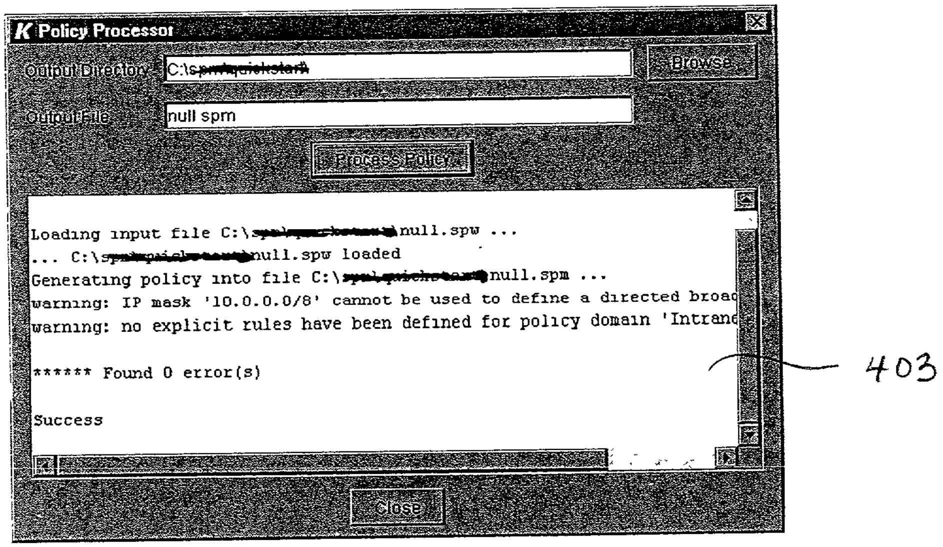


Policy Processor

Output Directory: C:\[redacted]

Output File: null spm

Fig. 4b



Output Directory: C:\s[redacted]

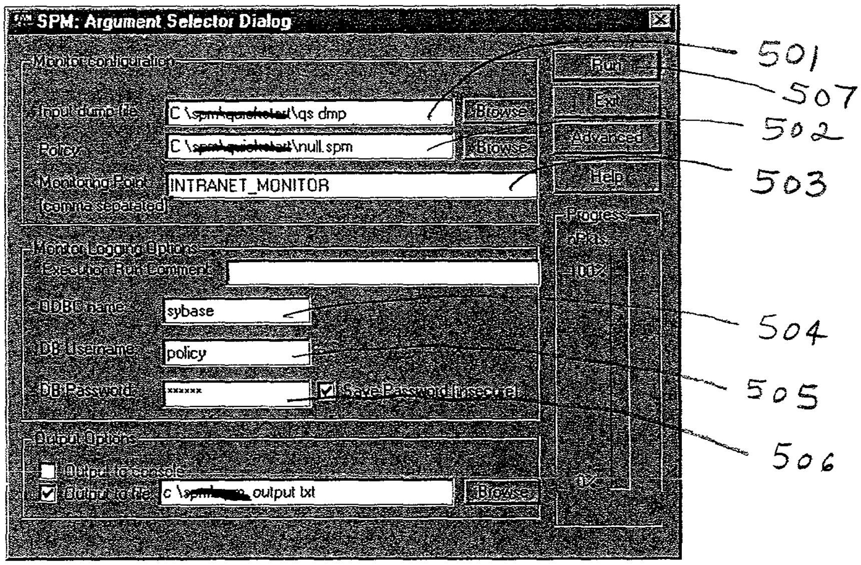
Output File: null spm

```
Loading input file C:\[redacted]null.spw ...
... C:\s[redacted]null.spw loaded
Generating policy into file C:\[redacted]null.spm ...
warning: IP mask '10.0.0.0/8' cannot be used to define a directed broac
warning: no explicit rules have been defined for policy domain 'Intrane

****** Found 0 error(s)

Success
```

Fig. 5



SPM: Argument Selector Dialog

Monitor configuration

Input dump file: C \[redacted]\qs dmp

Policy: C \[redacted]\null.spm

Monitoring Point (comma separated): INTRANET_MONITOR

Monitor Logging Options

Execution Run Comment:

ODBC name: sybase

DB Username: policy

DB Password: ****** ☑ Save Password (insecure)

Output Options

□ Output to console

☑ Output to file: c \[redacted] output txt

Fig. 6

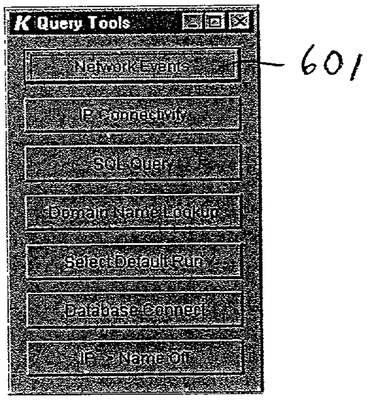
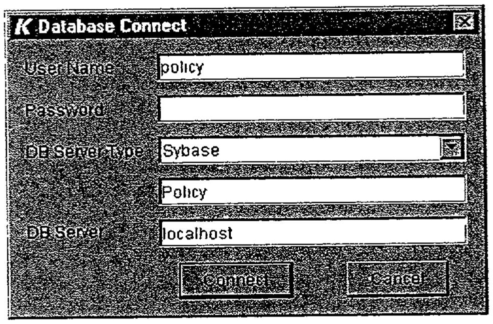

K Query Tools
Network Events
IP Connectivity
SQL Query
Domain Name Lookup
Select Default Run
Database Connect
IP -> Name Off
601

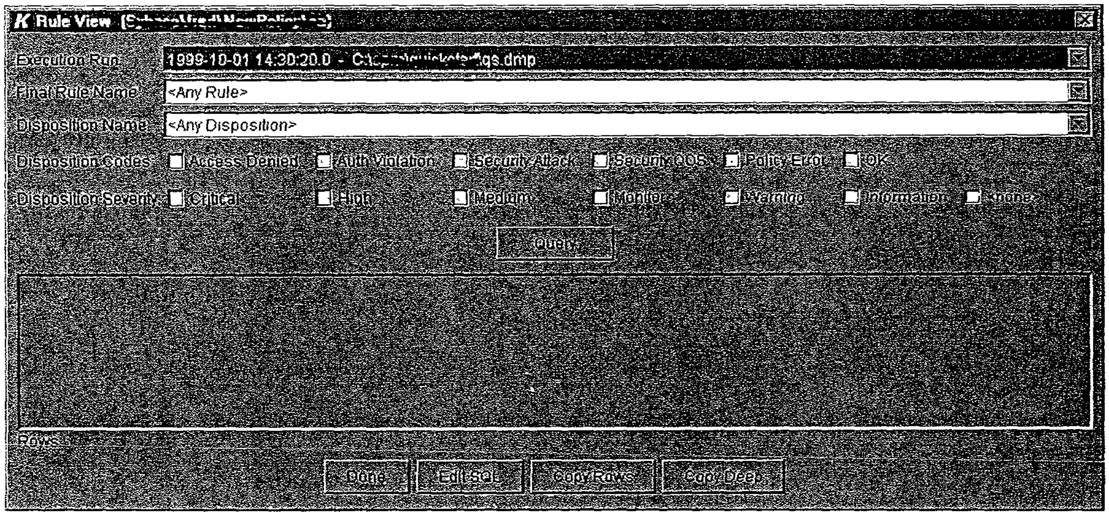
Fig. 7



Database Connect

User Name	policy
Password	
DB Server Type	Sybase
[illegible]	Policy
DB Server	localhost

Fig. 8



Rule View (S[illegible])

Execution Run: 1999-10-01 14:30:20.0 - C:\[illegible]qs.dmp

Final Rule Name: <Any Rule>

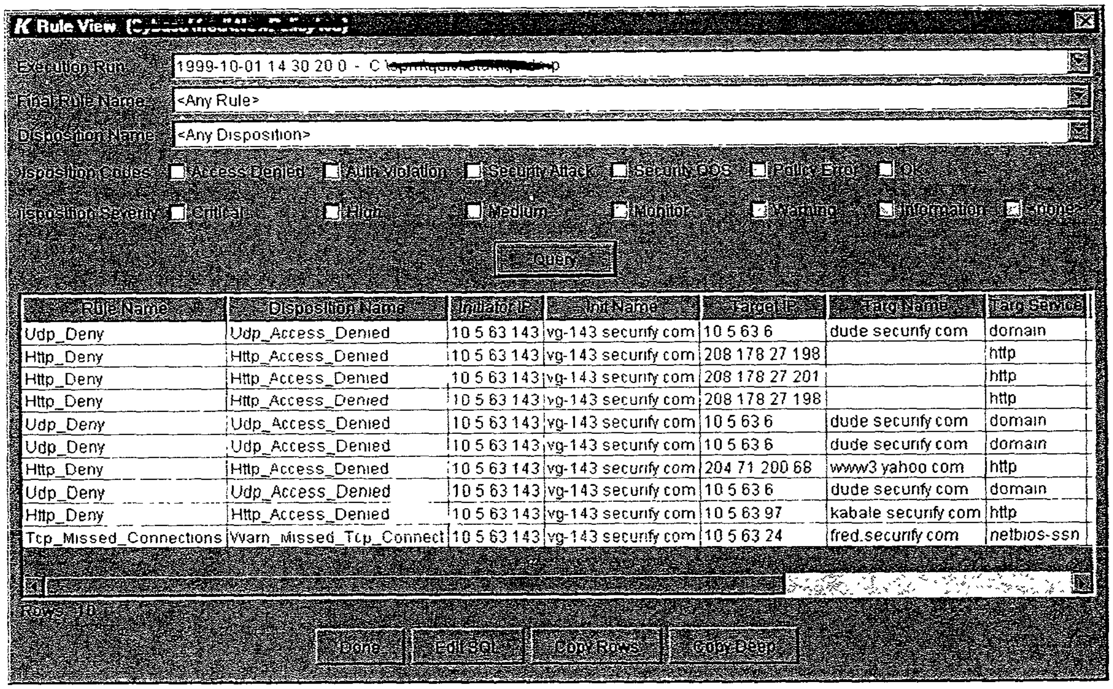
Disposition Name: <Any Disposition>

Disposition Codes: □ Access Denied ☑ Auth Violation □ Security Attack □ Security QOS ☑ Policy Error □ OK

Disposition Severity: □ Critical □ High □ Medium □ Monitor ☑ Warning □ Information □ <none>

Rows:

Fig. 9



Rule View [illegible]

Execution Run: 1999-10-01 14 30 20 0 - C [redacted] p

Final Rule Name: <Any Rule>

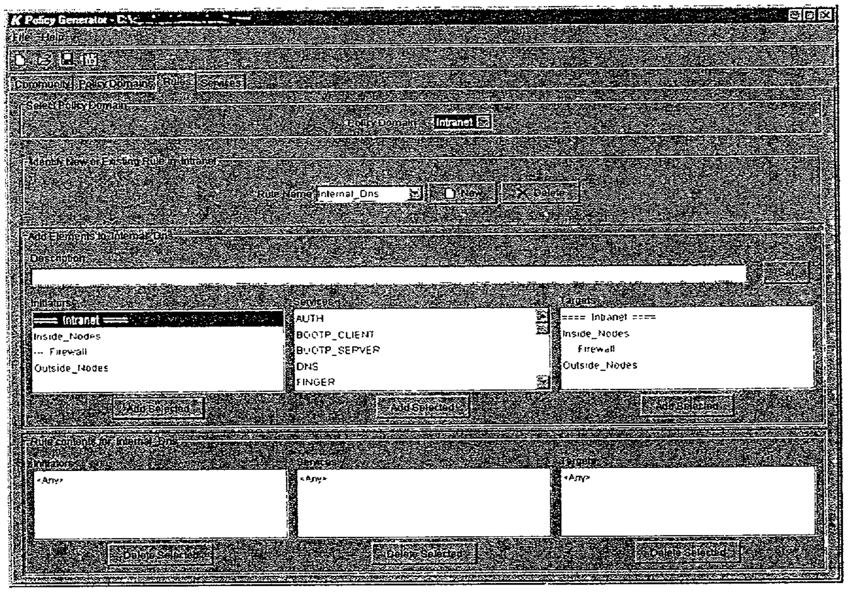
Disposition Name: <Any Disposition>

isposition Codes: ☐ Access Denied ☐ Auth Violation ☐ Security Attack ☐ Security DOS ☐ Policy Error ☐ OK

isposition Severity: ☐ Critical ☐ High ☐ Medium ☐ Monitor ☑ Warning ☑ Information ☑ <none>

Rule Name	Disposition Name	Initiator IP	Init Name	Target IP	Targ Name	Targ Service
Udp_Deny	Udp_Access_Denied	10 5 63 143	vg-143 securify com	10 5 63 6	dude securify com	domain
Http_Deny	Http_Access_Denied	10 5 63 143	vg-143 securify com	208 178 27 198		http
Http_Deny	Http_Access_Denied	10 5 63 143	vg-143 securify com	208 178 27 201		http
Http_Deny	Http_Access_Denied	10 5 63 143	vg-143 securify com	208 178 27 198		http
Udp_Deny	Udp_Access_Denied	10 5 63 143	vg-143 securify com	10 5 63 6	dude securify com	domain
Udp_Deny	Udp_Access_Denied	10 5 63 143	vg-143 securify com	10 5 63 6	dude securify com	domain
Http_Deny	Http_Access_Denied	10 5 63 143	vg-143 securify com	204 71 200 68	www3 yahoo com	http
Udp_Deny	Udp_Access_Denied	10 5 63 143	vg-143 securify com	10 5 63 6	dude securify com	domain
Http_Deny	Http_Access_Denied	10 5 63 143	vg-143 securify com	10 5 63 97	kabale securify com	http
Tcp_Missed_Connections	Warn_Missed_Tcp_Connect	10 5 63 143	vg-143 securify com	10 5 63 24	fred.securify com	netbios-ssn

Rows: 10



Select Policy Domain

Policy Domain: Intranet

Identify New or Existing Rule in Intranet

Rule Name: Internal_Dns

Add Elements to Internal_Dns

Description:

Initiators:
==== Intranet ====
Inside_Nodes
--- Firewall
Outside_Nodes

Services:
AUTH
BOOTP_CLIENT
BOOTP_SERVER
DNS
FINGER

Targets:
==== Intranet ====
Inside_Nodes
Firewall
Outside_Nodes

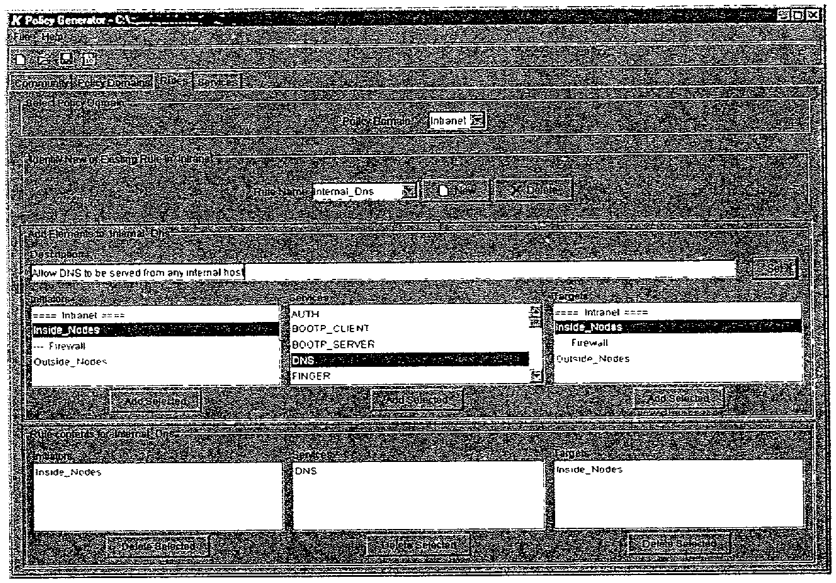
Rule contents for Internal_Dns

Initiators:
<Any>

Services:
<Any>

Targets:
<Any>

Fig. 10a


Policy Generator - C:\
File Help
Community | Policy Domains | Rules | Services
Select Policy Domain
Identify New or Existing Rule in Intranet
New
Delete
Add Elements to Internal_Dns
Set
Add Selected
Add Selected
Add Selected
Rule contents for Internal_Dns
Delete Selected
Delete Selected
Delete Selected

Policy Domain: Intranet

Rule Name: Internal_Dns

Description:

Allow DNS to be served from any internal host

Initiators:

```
==== Intranet ====
Inside_Nodes
--- Firewall
Outside_Nodes
```

Services:

```
AUTH
BOOTP_CLIENT
BOOTP_SERVER
DNS
FINGER
```

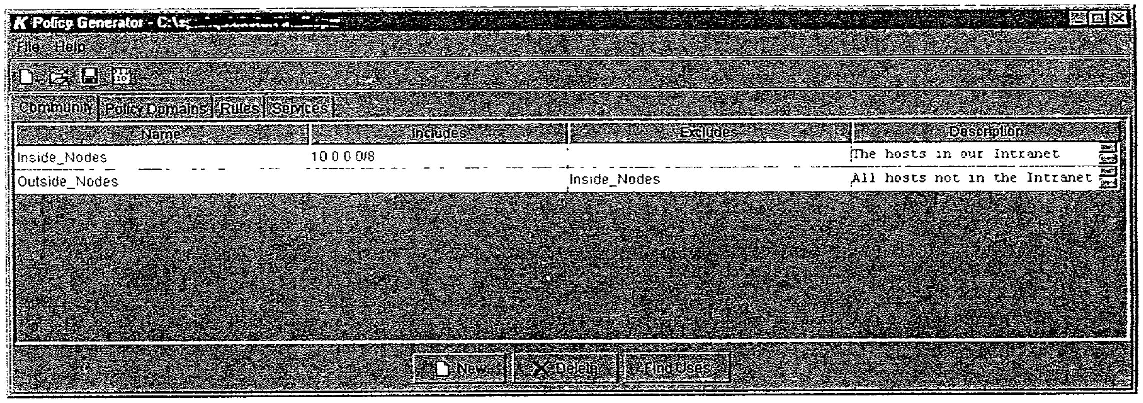
Targets:

```
==== Intranet ====
Inside_Nodes
    Firewall
Outside_Nodes
```

Rule contents for Internal_Dns

Initiators	Services	Targets
Inside_Nodes	DNS	Inside_Nodes

Fig. 10b



Name	Includes	Excludes	Description
Inside_Nodes	10 0 0 0/8		The hosts in our Intranet
Outside_Nodes		Inside_Nodes	All hosts not in the Intranet

Fig. 10c

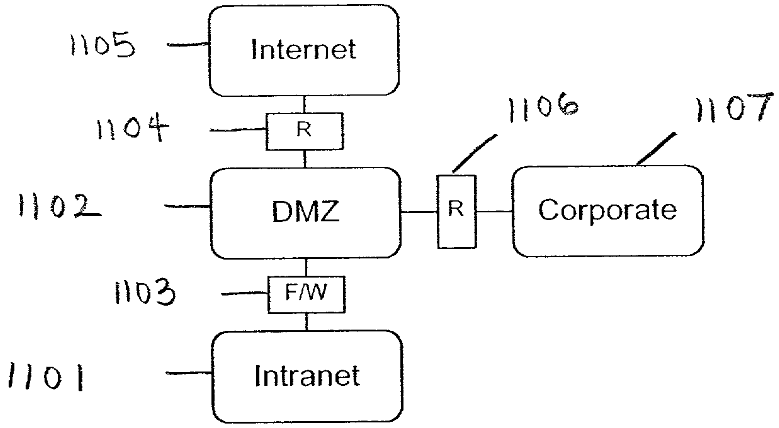
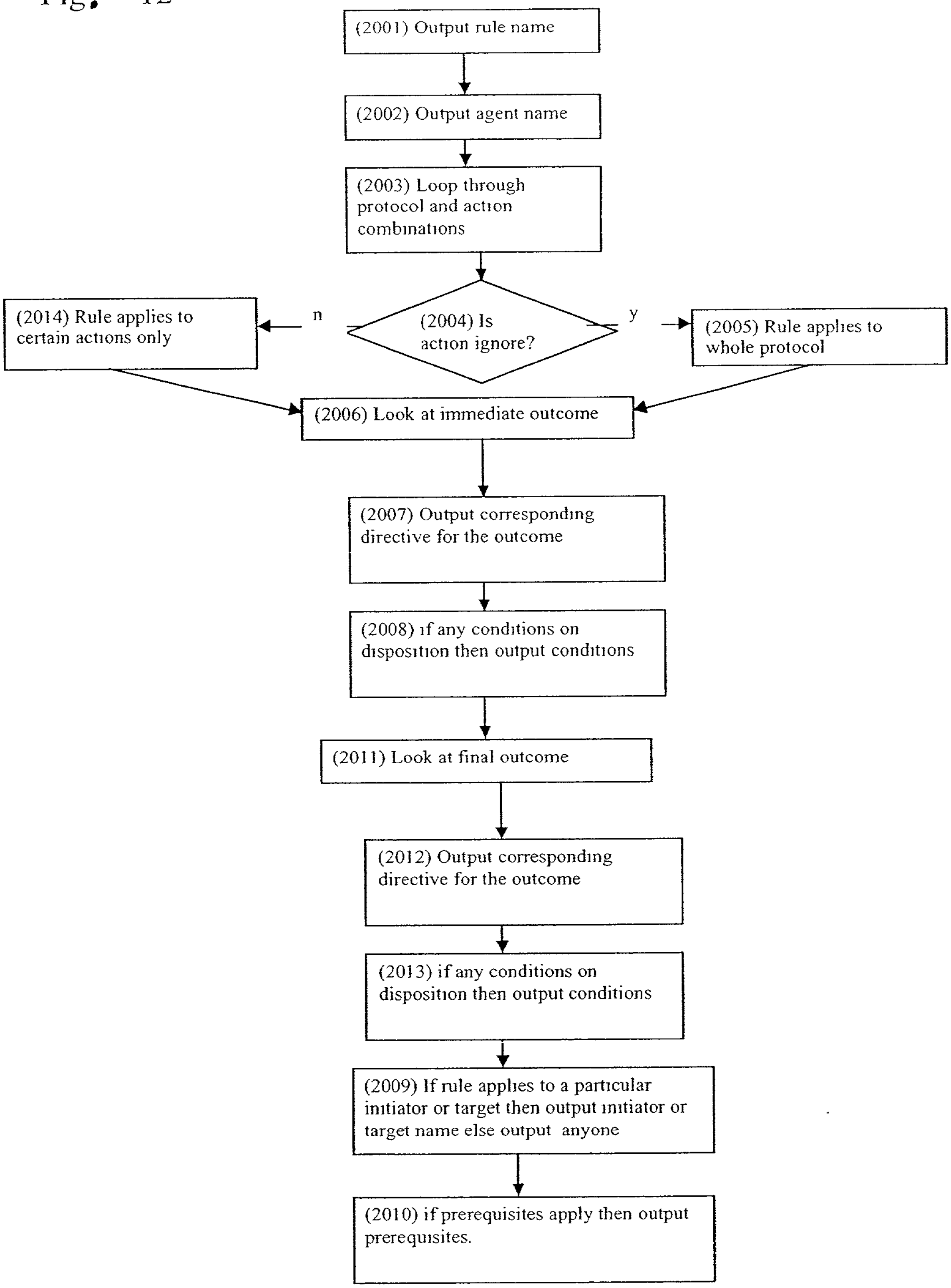
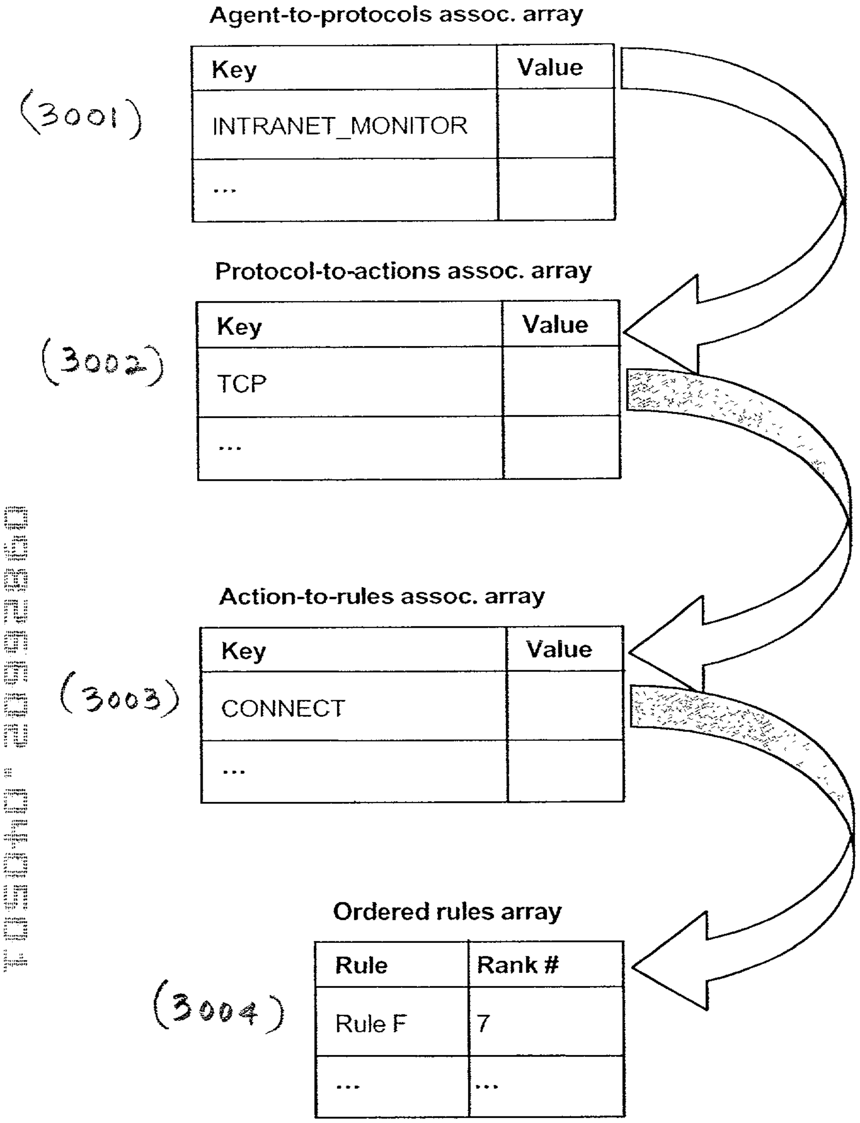

1105
Internet
1104
R
1106
1107
1102
DMZ
R
Corporate
1103
F/W
1101
Intranet

Fig. 11

Fig. 12


(2001) Output rule name
(2002) Output agent name
(2003) Loop through protocol and action combinations
(2004) Is action ignore?
n
y
(2014) Rule applies to certain actions only
(2005) Rule applies to whole protocol
(2006) Look at immediate outcome
(2007) Output corresponding directive for the outcome
(2008) if any conditions on disposition then output conditions
(2011) Look at final outcome
(2012) Output corresponding directive for the outcome
(2013) if any conditions on disposition then output conditions
(2009) If rule applies to a particular initiator or target then output initiator or target name else output anyone
(2010) if prerequisites apply then output prerequisites.



Agent-to-protocols assoc. array

Key	Value
INTRANET_MONITOR	
...	

Protocol-to-actions assoc. array

Key	Value
TCP	
...	

Action-to-rules assoc. array

Key	Value
CONNECT	
...	

Ordered rules array

Rule	Rank #
Rule F	7
...	...

Fig. 13

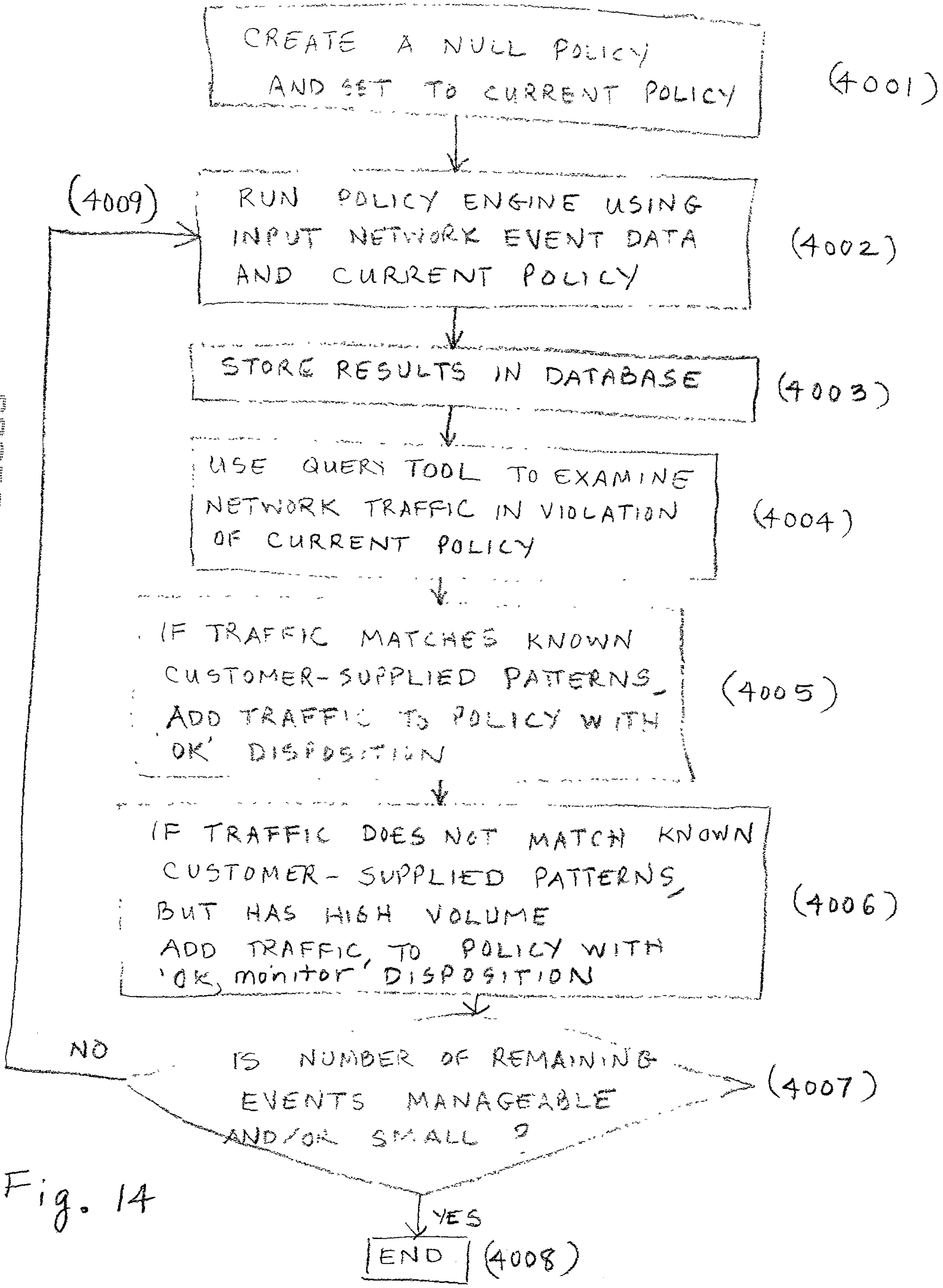

CREATE A NULL POLICY AND SET TO CURRENT POLICY
(4001)
(4009)
RUN POLICY ENGINE USING INPUT NETWORK EVENT DATA AND CURRENT POLICY
(4002)
STORE RESULTS IN DATABASE
(4003)
USE QUERY TOOL TO EXAMINE NETWORK TRAFFIC IN VIOLATION OF CURRENT POLICY
(4004)
IF TRAFFIC MATCHES KNOWN CUSTOMER-SUPPLIED PATTERNS, ADD TRAFFIC TO POLICY WITH 'OK' DISPOSITION
(4005)
IF TRAFFIC DOES NOT MATCH KNOWN CUSTOMER-SUPPLIED PATTERNS, BUT HAS HIGH VOLUME ADD TRAFFIC, TO POLICY WITH 'OK, monitor' DISPOSITION
(4006)
NO
IS NUMBER OF REMAINING EVENTS MANAGEABLE AND/OR SMALL ?
(4007)
YES
END
(4008)

Fig. 14

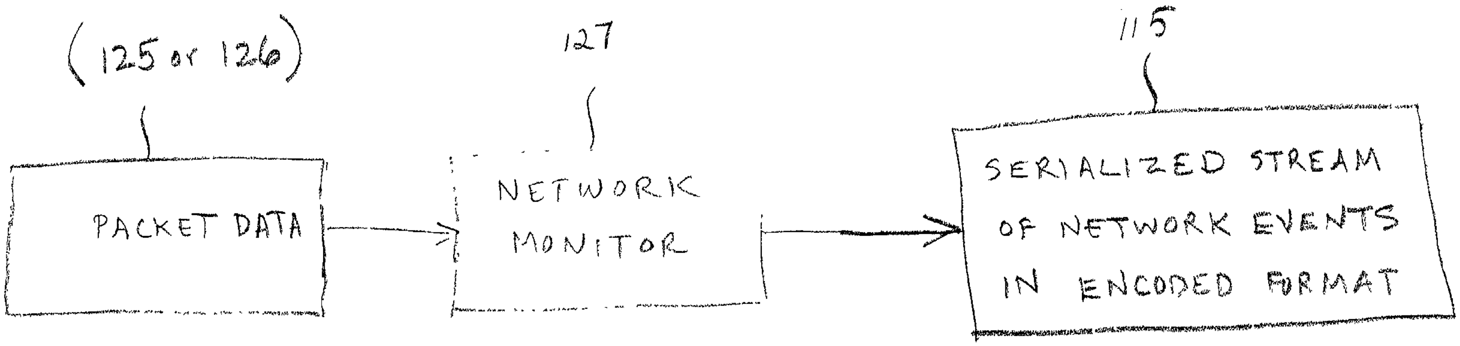

(125 or 126)
PACKET DATA
127
NETWORK MONITOR
115
SERIALIZED STREAM OF NETWORK EVENTS IN ENCODED FORMAT

Fig. 15

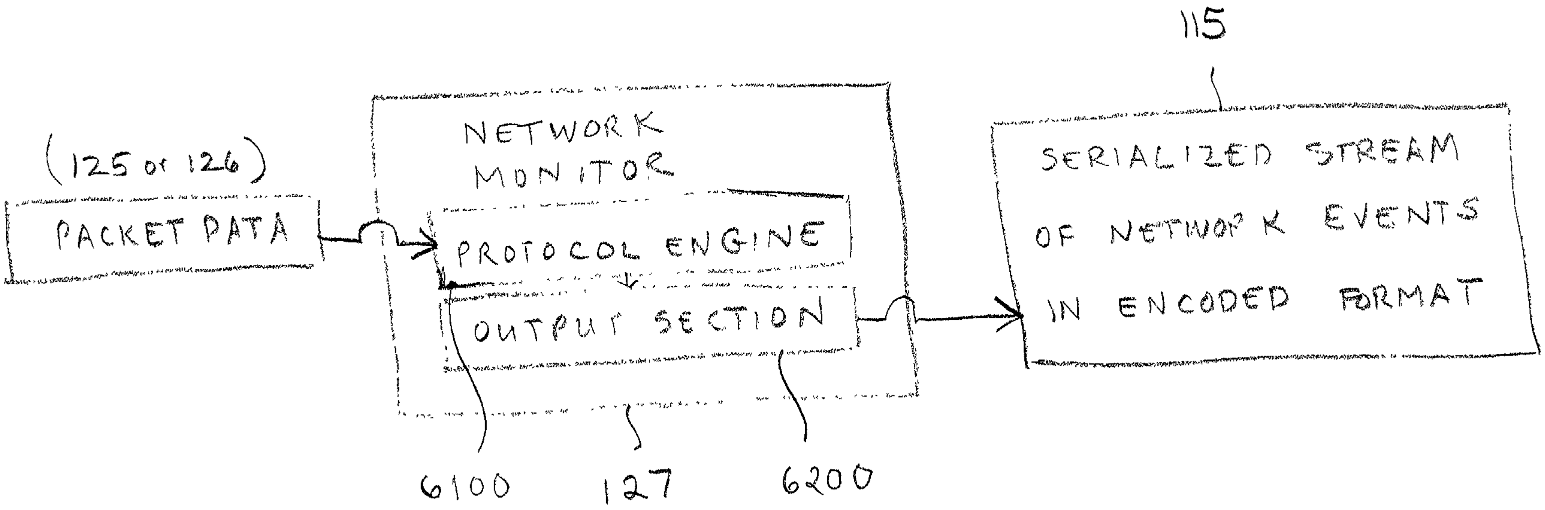

(125 or 126)
PACKET DATA
NETWORK MONITOR
PROTOCOL ENGINE
OUTPUT SECTION
6100
127
6200
115
SERIALIZED STREAM OF NETWORK EVENTS IN ENCODED FORMAT

Fig. 16

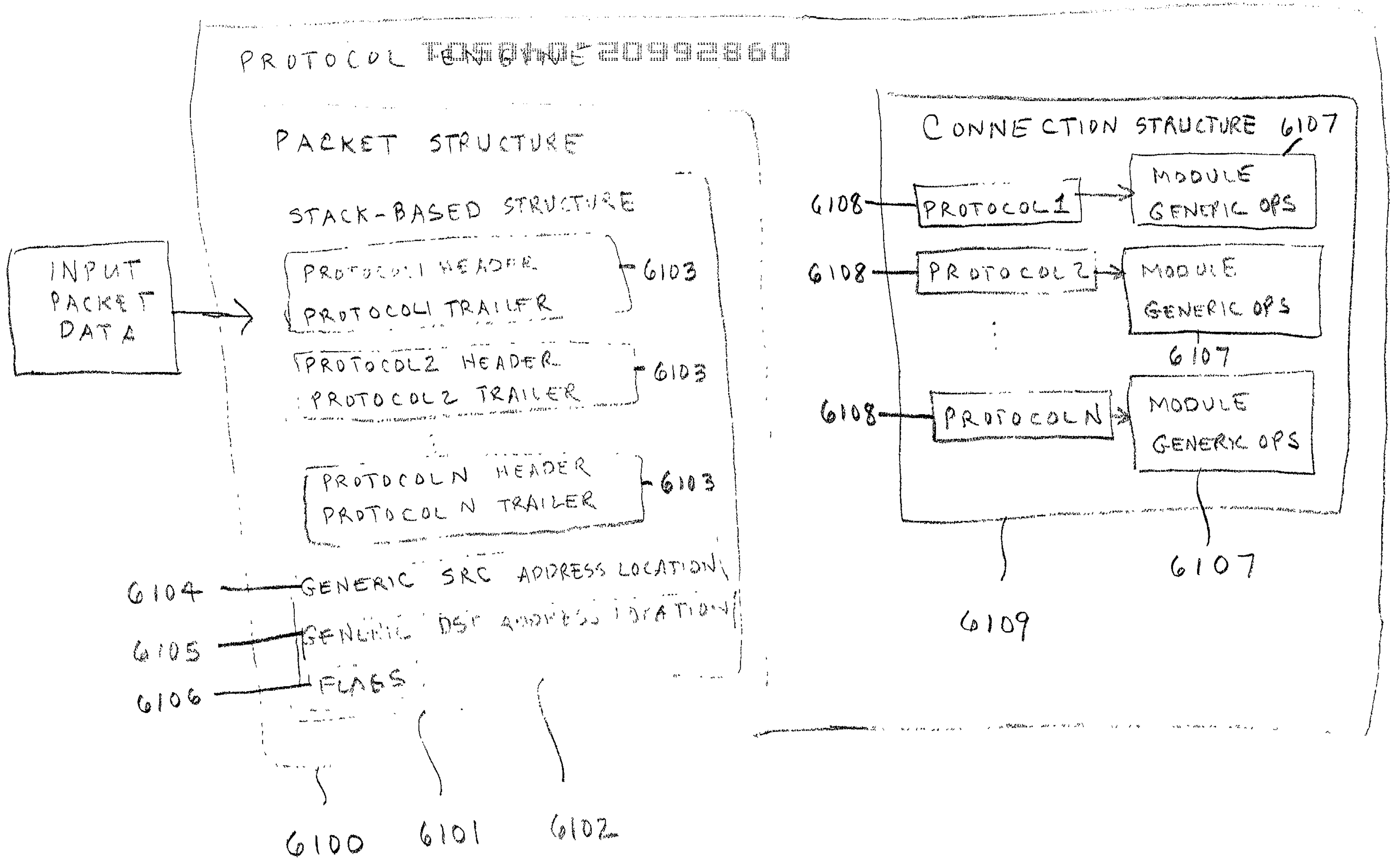

PROTOCOL ENGINE
PACKET STRUCTURE
STACK-BASED STRUCTURE
PROTOCOL1 HEADER
PROTOCOL1 TRAILER
6103
PROTOCOL2 HEADER
PROTOCOL2 TRAILER
6103
PROTOCOLN HEADER
PROTOCOL N TRAILER
6103
GENERIC SRC ADDRESS LOCATION
GENERIC DST ADDRESS LOCATION
FLAGS
6104
6105
6106
6100
6101
6102
INPUT PACKET DATA
CONNECTION STRUCTURE 6107
6108
PROTOCOL1
MODULE GENERIC OPS
6108
PROTOCOL2
MODULE GENERIC OPS
6107
6108
PROTOCOLN
MODULE GENERIC OPS
6107
6109

Fig. 17

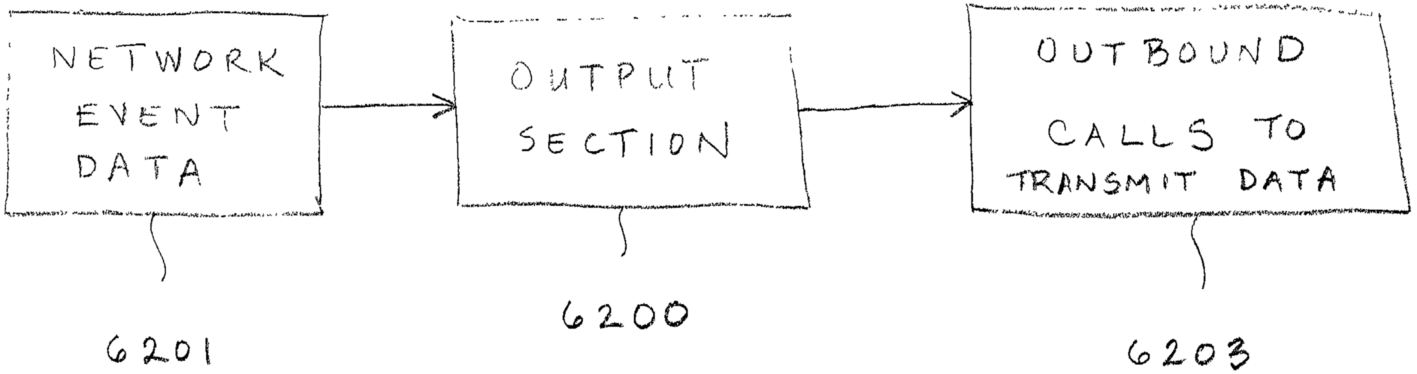

NETWORK EVENT DATA
OUTPUT SECTION
OUTBOUND CALLS TO TRANSMIT DATA
6201
6200
6203

Fig. 18

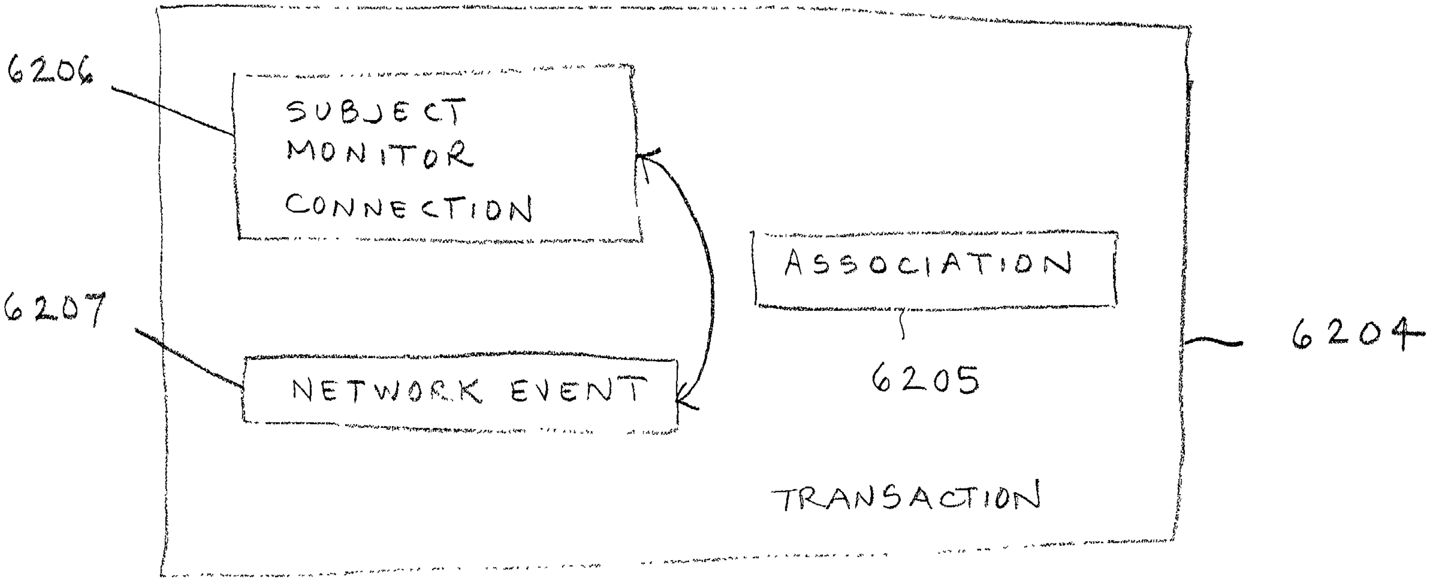
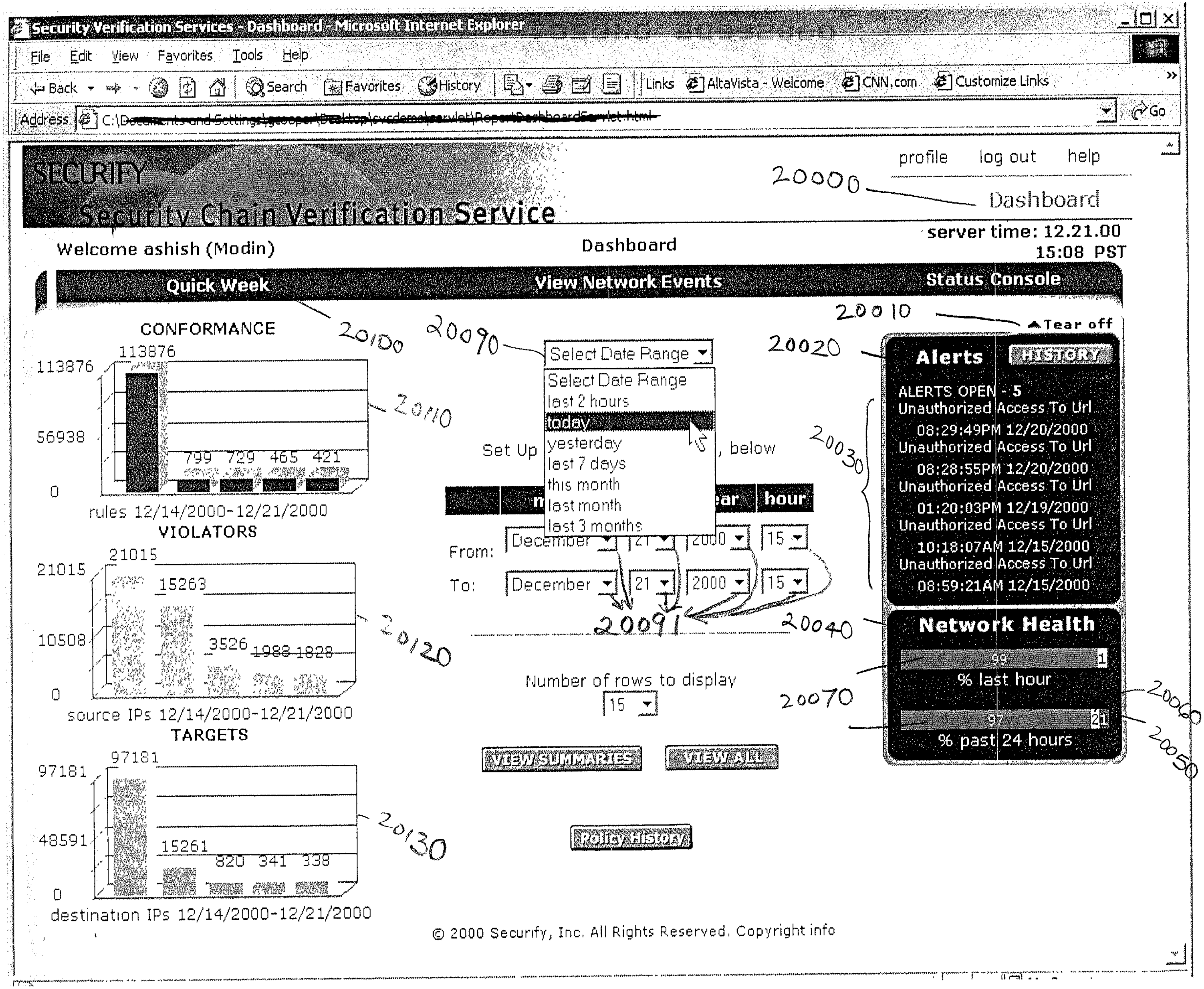

6206
SUBJECT MONITOR CONNECTION
6207
NETWORK EVENT
ASSOCIATION
6205
6204
TRANSACTION

Fig. 19



Security Verification Services - Dashboard - Microsoft Internet Explorer

File Edit View Favorites Tools Help
Back Search Favorites History Links AltaVista - Welcome CNN.com Customize Links
Go

Address C:\[redacted]

SECURIFY
Security Chain Verification Service

profile log out help

Dashboard

server time: 12.21.00 15:08 PST

Welcome ashish (Modin)

Dashboard

CONFORMANCE

rules 12/14/2000-12/21/2000

VIOLATORS

source IPs 12/14/2000-12/21/2000

TARGETS

destination IPs 12/14/2000-12/21/2000

Select Date Range

Set Up , below

From: December 21 2000 15

To: December 21 2000 15

Number of rows to display 15

Alerts

ALERTS OPEN - 5

Unauthorized Access To Url 08:29:49PM 12/20/2000

Unauthorized Access To Url 08:28:55PM 12/20/2000

Unauthorized Access To Url 01:20:03PM 12/19/2000

Unauthorized Access To Url 10:18:07AM 12/15/2000

Unauthorized Access To Url 08:59:21AM 12/15/2000

Network Health

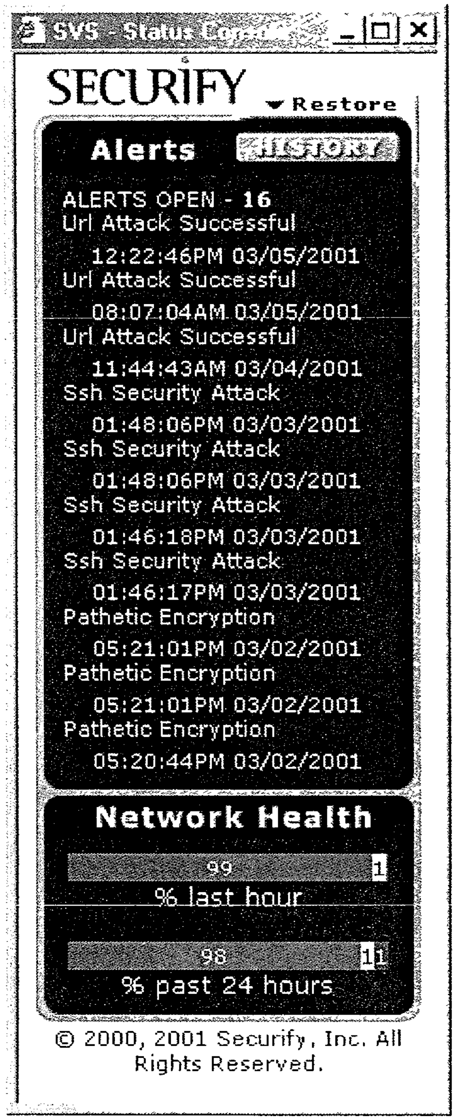
% last hour

% past 24 hours

© 2000 Securify, Inc. All Rights Reserved. Copyright info

Fig. 20

~~This is a screen shot of the tear-off status console. On the main page (Dashboard) if you click on the tear-off tab then this window is opened. It is intended that the user could keep this open on their computer all day to receive a high level view of the health of their network.~~



ALERTS OPEN - **16**
Url Attack Successful
12:22:46PM 03/05/2001
Url Attack Successful
08:07:04AM 03/05/2001
Url Attack Successful
11:44:43AM 03/04/2001
Ssh Security Attack
01:48:06PM 03/03/2001
Ssh Security Attack
01:48:06PM 03/03/2001
Ssh Security Attack
01:46:18PM 03/03/2001
Ssh Security Attack
01:46:17PM 03/03/2001
Pathetic Encryption
05:21:01PM 03/02/2001
Pathetic Encryption
05:21:01PM 03/02/2001
Pathetic Encryption
05:20:44PM 03/02/2001

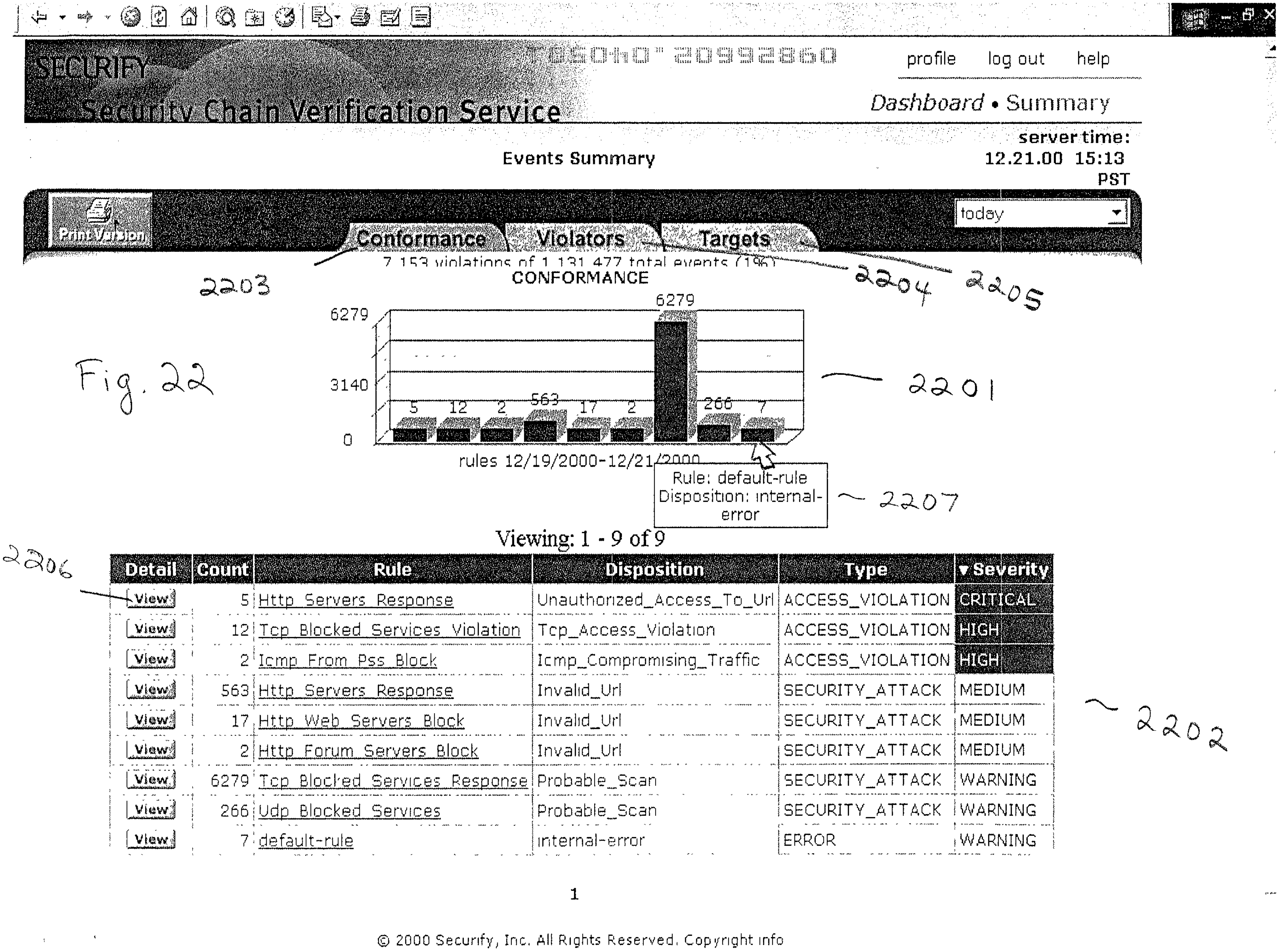
Network Health

99 1
% last hour

98 11
% past 24 hours

© 2000, 2001 Securify, Inc. All Rights Reserved.

Fig. 21



server time: 12.21.00 15:13 PST

Events Summary

7 153 violations of 1 131 477 total events (1%)

Rule: default-rule
Disposition: internal-error

Viewing: 1 - 9 of 9

Detail	Count	Rule	Disposition	Type	▾ Severity
View	5	Http_Servers_Response	Unauthorized_Access_To_Url	ACCESS_VIOLATION	CRITICAL
View	12	Tcp_Blocked_Services_Violation	Tcp_Access_Violation	ACCESS_VIOLATION	HIGH
View	2	Icmp_From_Pss_Block	Icmp_Compromising_Traffic	ACCESS_VIOLATION	HIGH
View	563	Http_Servers_Response	Invalid_Url	SECURITY_ATTACK	MEDIUM
View	17	Http_Web_Servers_Block	Invalid_Url	SECURITY_ATTACK	MEDIUM
View	2	Http_Forum_Servers_Block	Invalid_Url	SECURITY_ATTACK	MEDIUM
View	6279	Tcp_Blocked_Services_Response	Probable_Scan	SECURITY_ATTACK	WARNING
View	266	Udp_Blocked_Services	Probable_Scan	SECURITY_ATTACK	WARNING
View	7	default-rule	internal-error	ERROR	WARNING

1

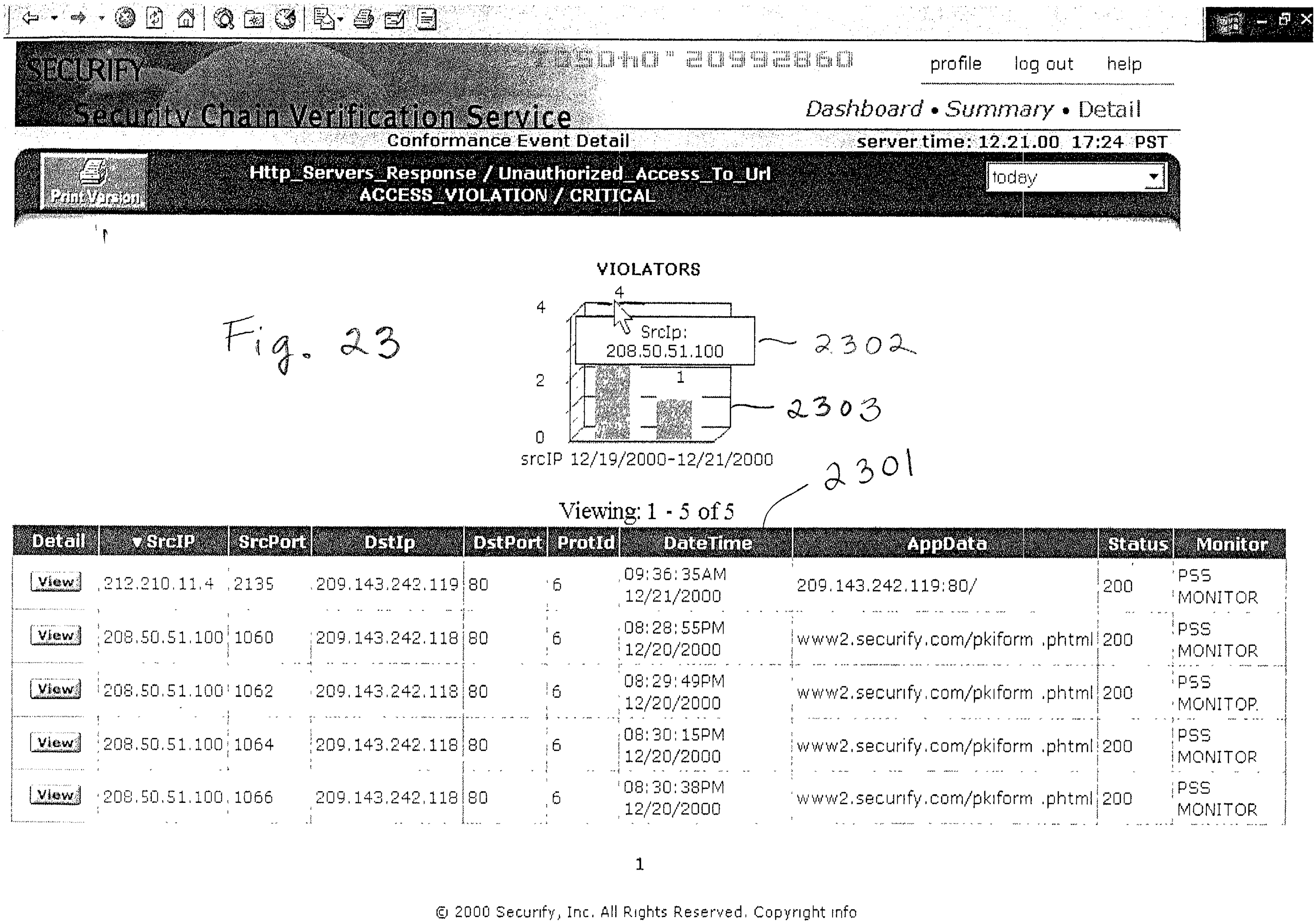


Fig. 23

Security Chain Verification Service

Conformance Event Detail

server time: 12.21.00 17:24 PST

Http_Servers_Response / Unauthorized_Access_To_Url
ACCESS_VIOLATION / CRITICAL

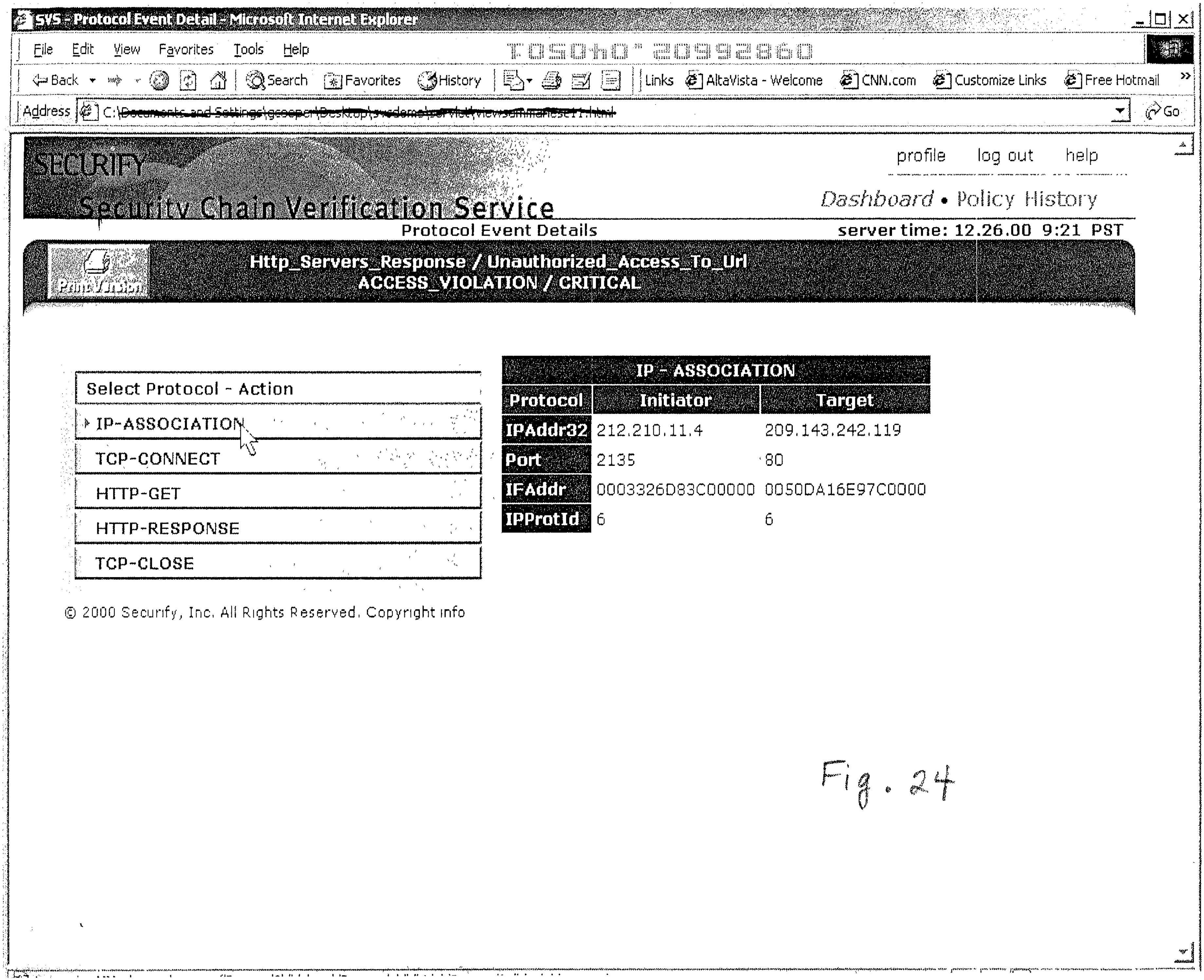
srcIP 12/19/2000-12/21/2000

Viewing: 1 - 5 of 5

Detail	▼SrcIP	SrcPort	DstIp	DstPort	ProtId	DateTime	AppData	Status	Monitor
View	212.210.11.4	2135	209.143.242.119	80	6	09:36:35AM 12/21/2000	209.143.242.119:80/	200	PSS MONITOR
View	208.50.51.100	1060	209.143.242.118	80	6	08:28:55PM 12/20/2000	www2.securify.com/pkiform .phtml	200	PSS MONITOR
View	208.50.51.100	1062	209.143.242.118	80	6	08:29:49PM 12/20/2000	www2.securify.com/pkiform .phtml	200	PSS MONITOR
View	208.50.51.100	1064	209.143.242.118	80	6	08:30:15PM 12/20/2000	www2.securify.com/pkiform .phtml	200	PSS MONITOR
View	208.50.51.100	1066	209.143.242.118	80	6	08:30:38PM 12/20/2000	www2.securify.com/pkiform .phtml	200	PSS MONITOR

1

© 2000 Securify, Inc. All Rights Reserved. Copyright info



SVS - Protocol Event Detail - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History Links AltaVista - Welcome CNN.com Customize Links Free Hotmail
Go
SECURIFY
profile log out help
Print Version

Address C:\~~Documents and Settings\gcooper\Desktop\svsdemo\servlet\viewsummaries11.html~~

Security Chain Verification Service

Dashboard • Policy History

Protocol Event Details

server time: 12.26.00 9:21 PST

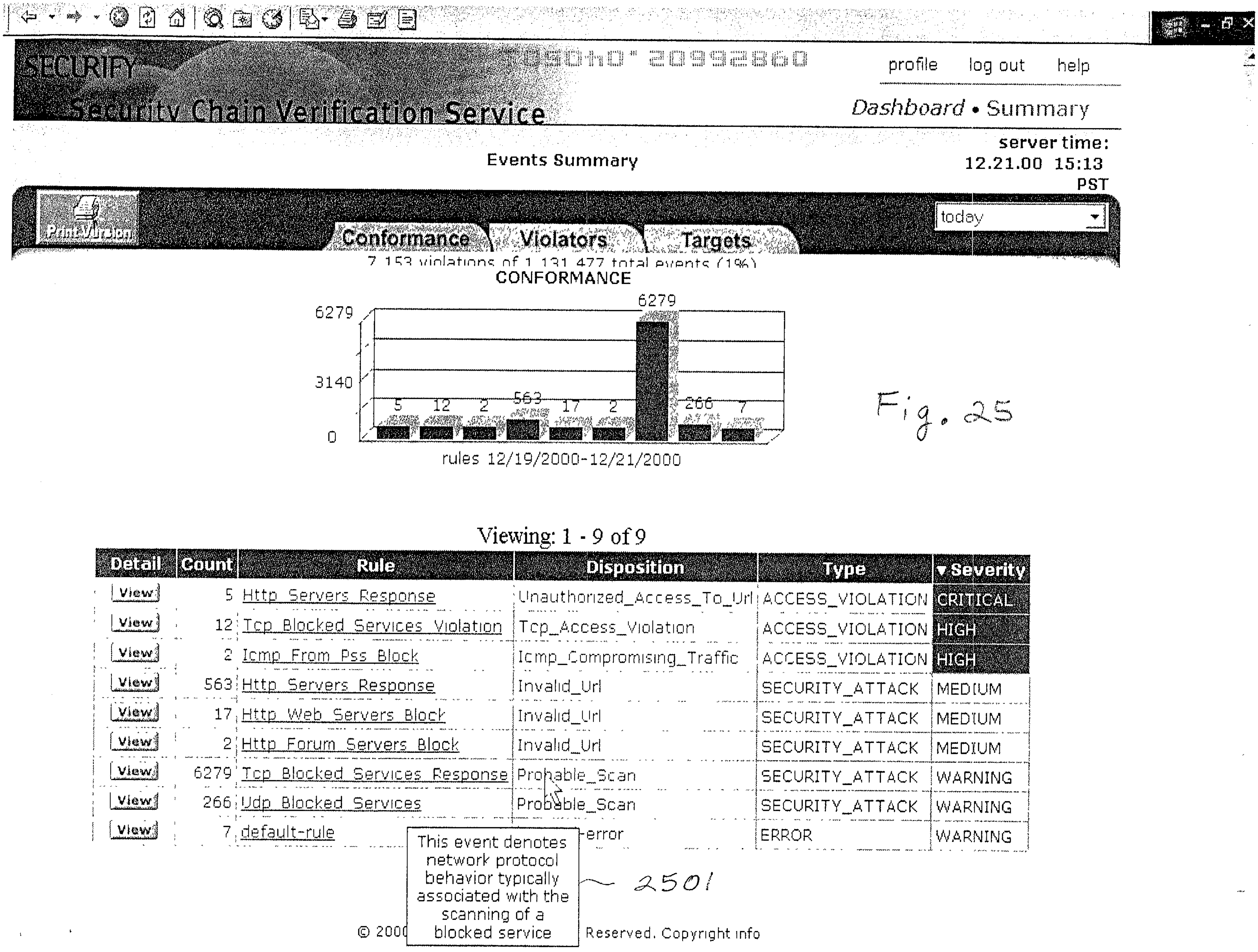
Http_Servers_Response / Unauthorized_Access_To_Url
ACCESS_VIOLATION / CRITICAL

Select Protocol - Action

- IP-ASSOCIATION
- TCP-CONNECT
- HTTP-GET
- HTTP-RESPONSE
- TCP-CLOSE

IP - ASSOCIATION		
Protocol	Initiator	Target
IPAddr32	212.210.11.4	209.143.242.119
Port	2135	80
IFAddr	0003326D83C00000	0050DA16E97C0000
IPProtId	6	6

Fig. 24



Dashboard • Summary

server time:
12.21.00 15:13
PST

Events Summary

7 153 violations of 1 131 477 total events (1%)

CONFORMANCE

rules 12/19/2000-12/21/2000

Fig. 25

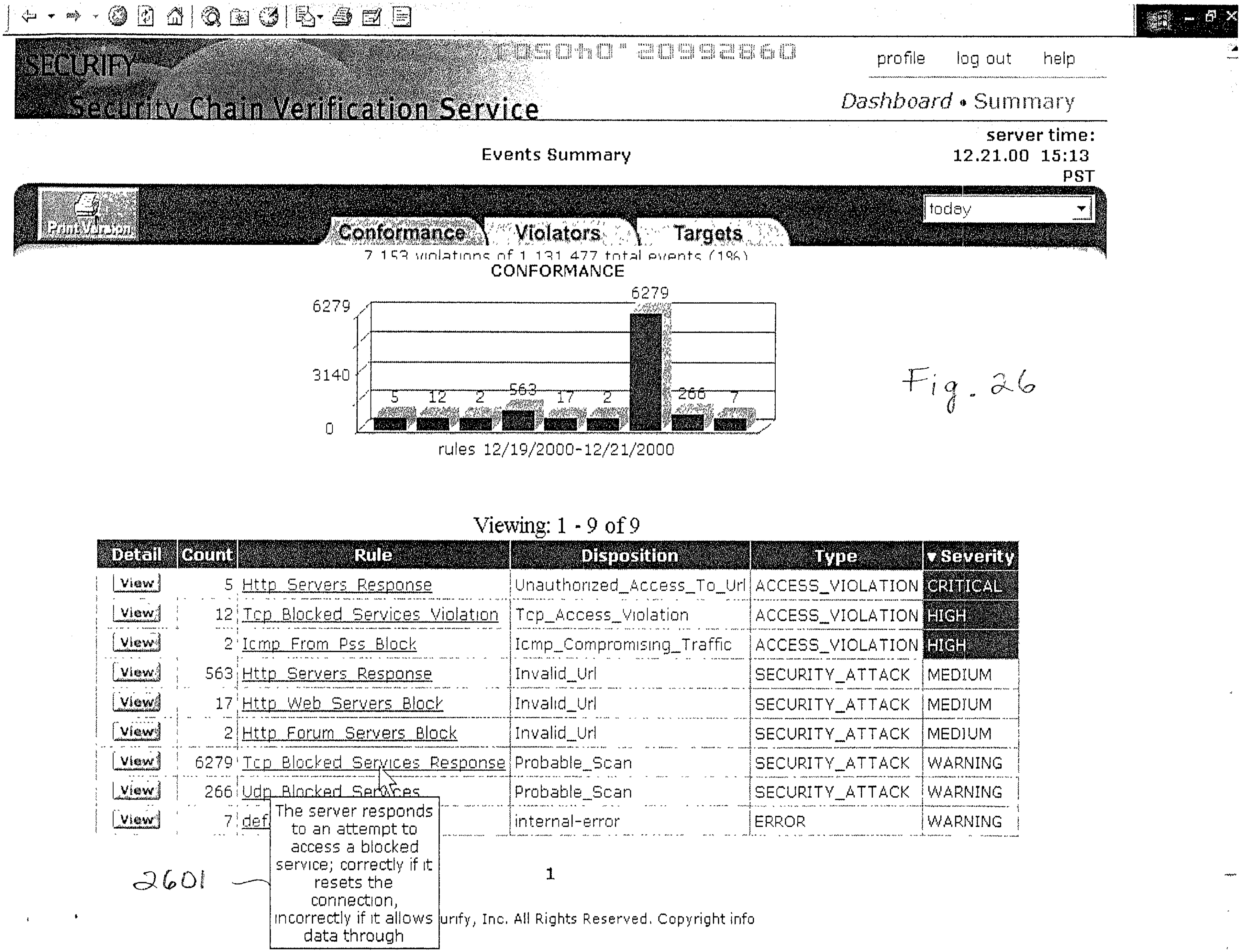
Viewing: 1 - 9 of 9

Detail	Count	Rule	Disposition	Type	▾ Severity
View	5	Http_Servers_Response	Unauthorized_Access_To_Url	ACCESS_VIOLATION	CRITICAL
View	12	Tcp_Blocked_Services_Violation	Tcp_Access_Violation	ACCESS_VIOLATION	HIGH
View	2	Icmp_From_Pss_Block	Icmp_Compromising_Traffic	ACCESS_VIOLATION	HIGH
View	563	Http_Servers_Response	Invalid_Url	SECURITY_ATTACK	MEDIUM
View	17	Http_Web_Servers_Block	Invalid_Url	SECURITY_ATTACK	MEDIUM
View	2	Http_Forum_Servers_Block	Invalid_Url	SECURITY_ATTACK	MEDIUM
View	6279	Tcp_Blocked_Services_Response	Probable_Scan	SECURITY_ATTACK	WARNING
View	266	Udp_Blocked_Services	Probable_Scan	SECURITY_ATTACK	WARNING
View	7	default-rule	error	ERROR	WARNING

This event denotes network protocol behavior typically associated with the scanning of a blocked service

2501

© 2000 Reserved. Copyright info



Events Summary

server time:
12.21.00 15:13
PST

7 153 violations of 1 131 477 total events (1%)

Viewing: 1 - 9 of 9

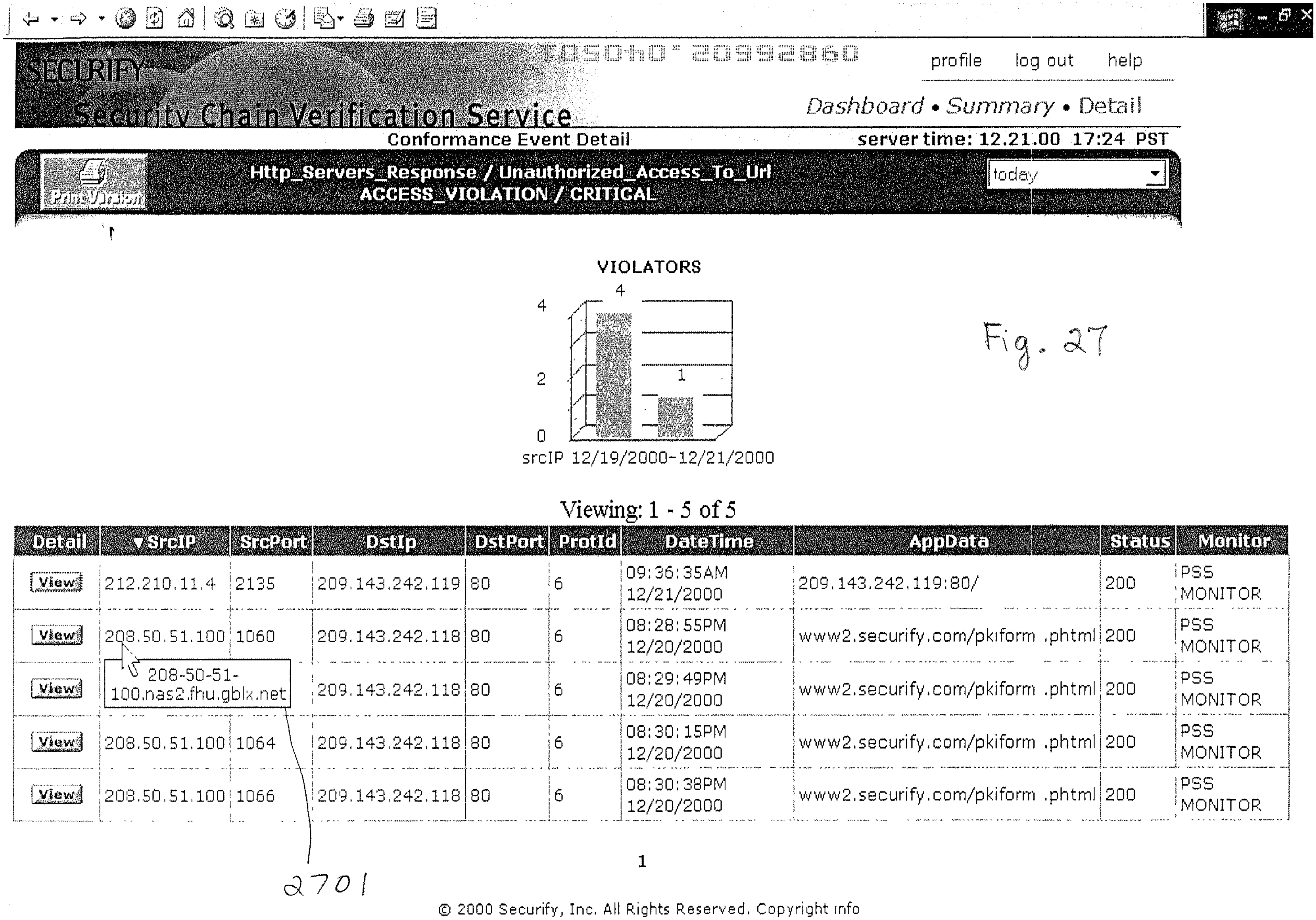
Detail	Count	Rule	Disposition	Type	▾Severity
View	5	Http Servers Response	Unauthorized_Access_To_Url	ACCESS_VIOLATION	CRITICAL
View	12	Tcp Blocked Services Violation	Tcp_Access_Violation	ACCESS_VIOLATION	HIGH
View	2	Icmp From Pss Block	Icmp_Compromising_Traffic	ACCESS_VIOLATION	HIGH
View	563	Http Servers Response	Invalid_Url	SECURITY_ATTACK	MEDIUM
View	17	Http Web Servers Block	Invalid_Url	SECURITY_ATTACK	MEDIUM
View	2	Http Forum Servers Block	Invalid_Url	SECURITY_ATTACK	MEDIUM
View	6279	Tcp Blocked Services Response	Probable_Scan	SECURITY_ATTACK	WARNING
View	266	Udp Blocked Services	Probable_Scan	SECURITY_ATTACK	WARNING
View	7	def	internal-error	ERROR	WARNING

The server responds to an attempt to access a blocked service; correctly if it resets the connection, incorrectly if it allows data through

1

urify, Inc. All Rights Reserved. Copyright info

Fig. 26



SECURIFY
Security Chain Verification Service
profile
log out
help
Dashboard • Summary • Detail
Print Version
today
VIOLATORS
4
2
0
4
1
srcIP 12/19/2000-12/21/2000
208-50-51-100.nas2.fhu.gblx.net
2701

Conformance Event Detail

server time: 12.21.00 17:24 PST

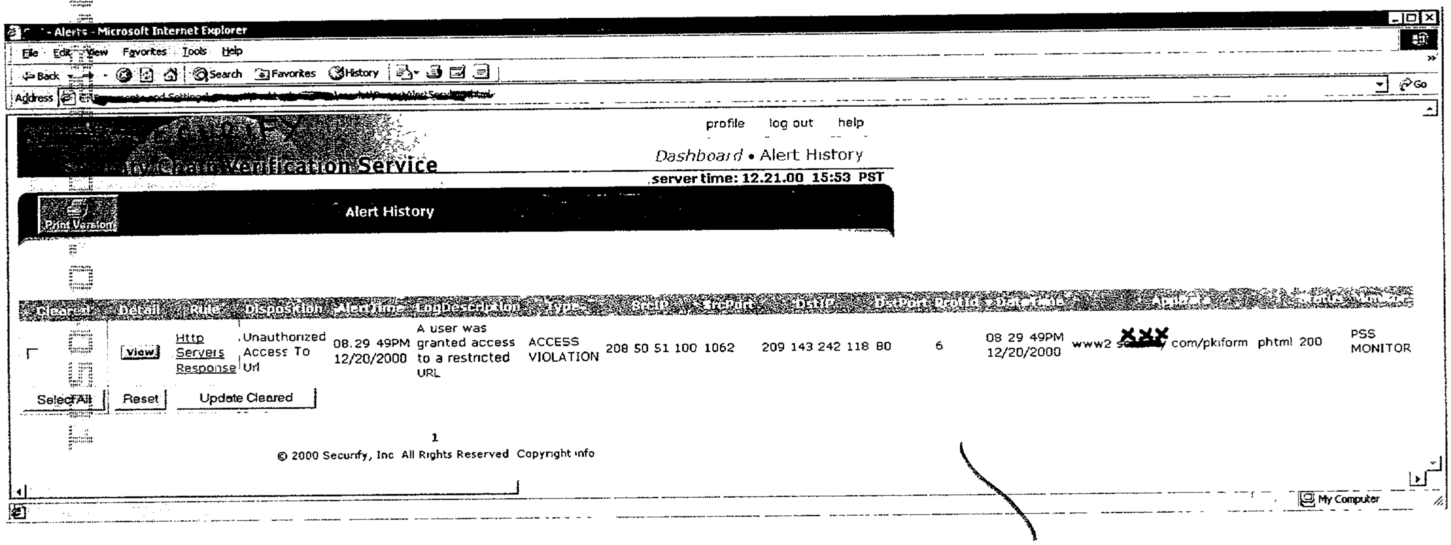
Http_Servers_Response / Unauthorized_Access_To_Url
ACCESS_VIOLATION / CRITICAL

Viewing: 1 - 5 of 5

Detail	▼SrcIP	SrcPort	DstIp	DstPort	ProtId	DateTime	AppData	Status	Monitor
View	212.210.11.4	2135	209.143.242.119	80	6	09:36:35AM 12/21/2000	209.143.242.119:80/	200	PSS MONITOR
View	208.50.51.100	1060	209.143.242.118	80	6	08:28:55PM 12/20/2000	www2.securify.com/pkiform .phtml	200	PSS MONITOR
View			209.143.242.118	80	6	08:29:49PM 12/20/2000	www2.securify.com/pkiform .phtml	200	PSS MONITOR
View	208.50.51.100	1064	209.143.242.118	80	6	08:30:15PM 12/20/2000	www2.securify.com/pkiform .phtml	200	PSS MONITOR
View	208.50.51.100	1066	209.143.242.118	80	6	08:30:38PM 12/20/2000	www2.securify.com/pkiform .phtml	200	PSS MONITOR

1

Fig. 27


Alerts - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address [redacted]
Go
profile log out help
Print Version
Select All
Reset
Update Cleared
My Computer

Verification Service

Dashboard • Alert History

server time: 12.21.00 15:53 PST

Alert History

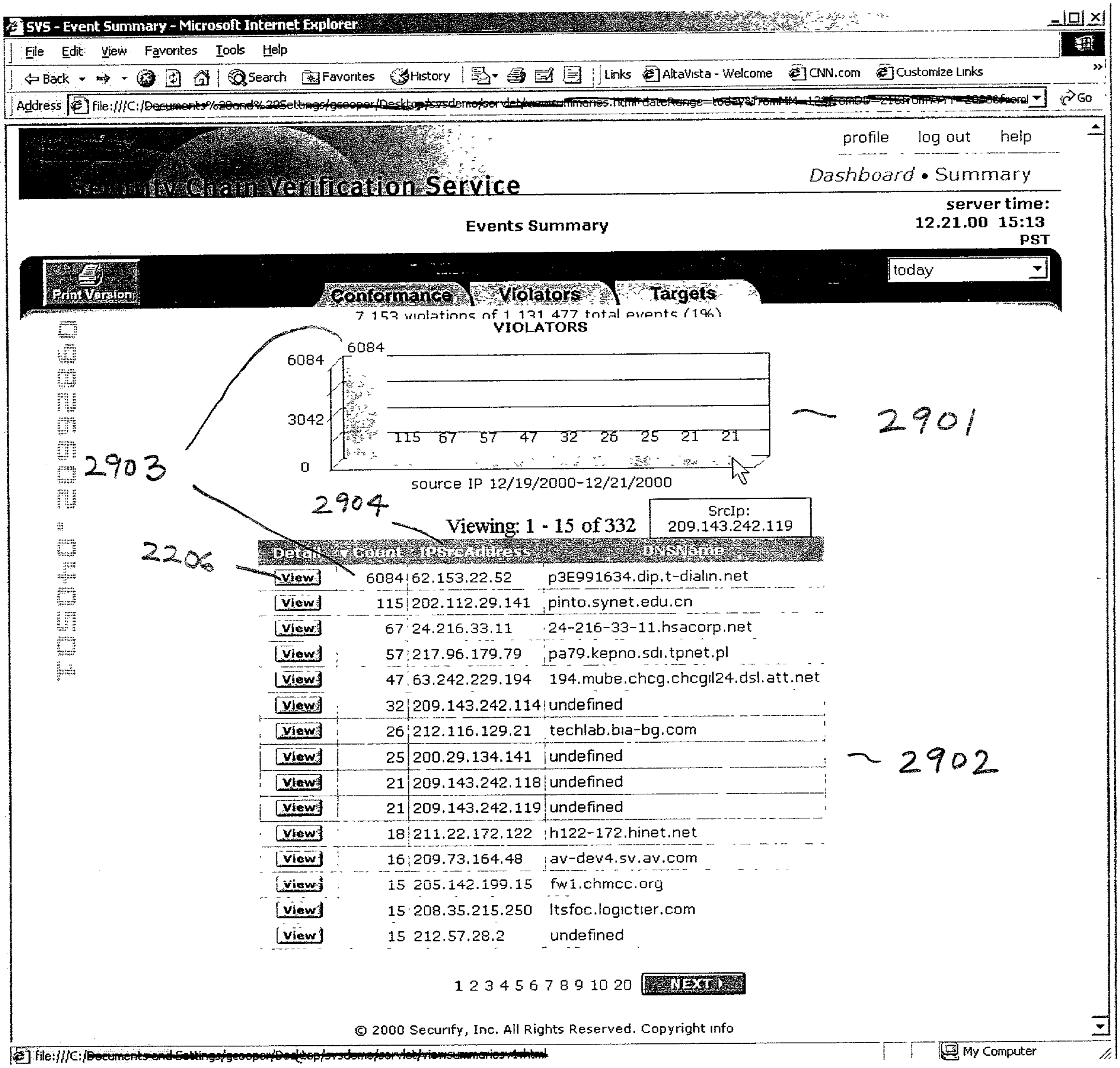
Cleared	Detail	Rule	Disposition	AlertTime	LogDescription	Type	SrcIP	SrcPort	DstIP	DstPort	ProtId	DateTime	[illegible]	Status	[illegible]
□	View	Http Servers Response	Unauthorized Access To Url	08.29 49PM 12/20/2000	A user was granted access to a restricted URL	ACCESS VIOLATION	208 50 51 100	1062	209 143 242 118	80	6	08 29 49PM 12/20/2000	www2 [redacted] com/pkiform phtml	200	PSS MONITOR

1

© 2000 Securify, Inc All Rights Reserved Copyright info

Fig. 28

2801



Address: file:///C:/~~Documents%20and%20Settings/gcooper/Desktop/svsdemo/servlet/viewsummaries~~.html?dateRange=~~today&fromMM=12&fromDD=21&fromYYYY=2000&toMM~~

server time:
12.21.00 15:13
PST

Events Summary

7,153 violations of 1,131,477 total events (1%)

Viewing: 1 - 15 of 332

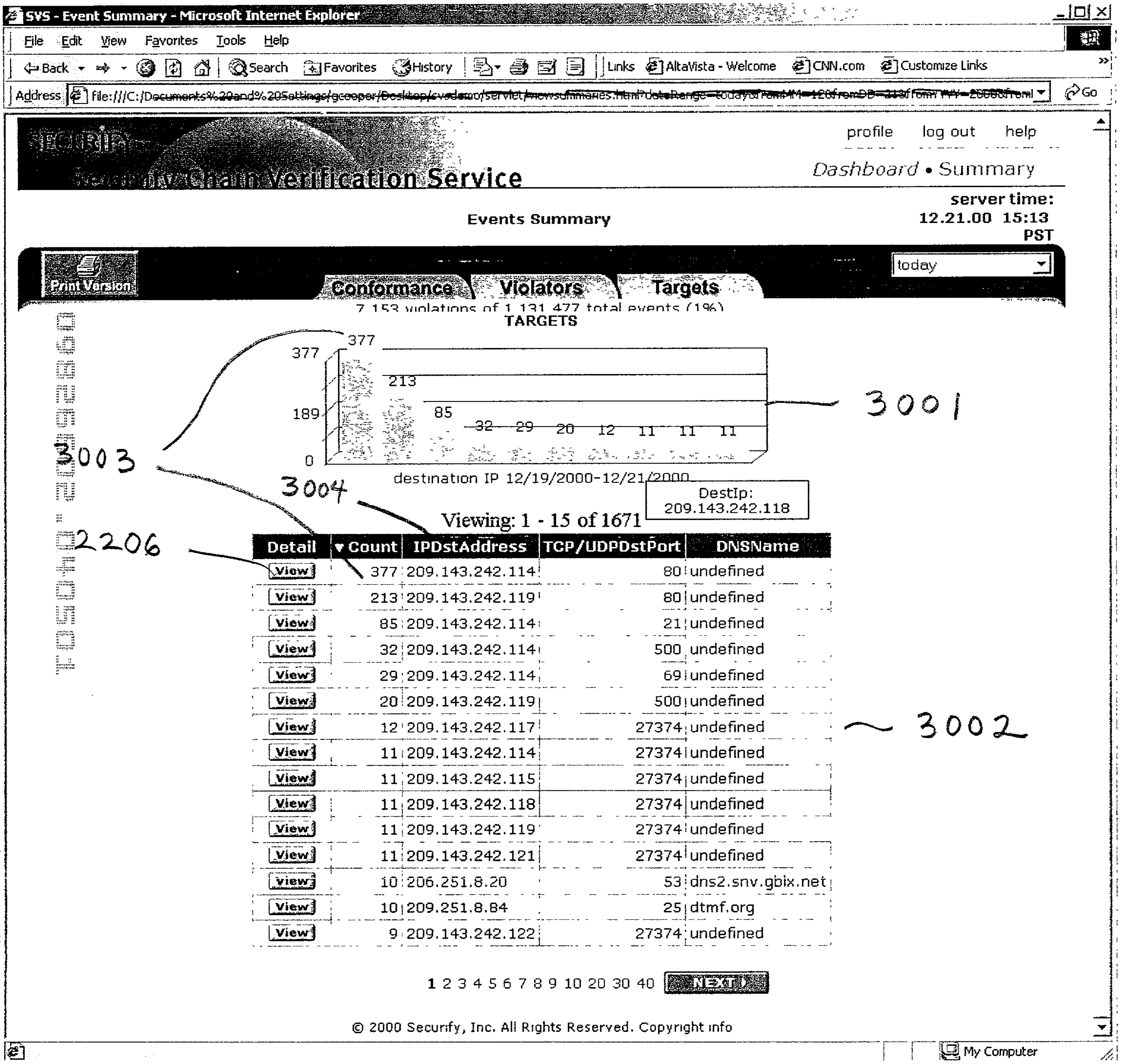
SrcIp:
209.143.242.119

Detail	▼Count	IPSrcAddress	DNSName
View	6084	62.153.22.52	p3E991634.dip.t-dialin.net
View	115	202.112.29.141	pinto.synet.edu.cn
View	67	24.216.33.11	24-216-33-11.hsacorp.net
View	57	217.96.179.79	pa79.kepno.sdi.tpnet.pl
View	47	63.242.229.194	194.mube.chcg.chcgil24.dsl.att.net
View	32	209.143.242.114	undefined
View	26	212.116.129.21	techlab.bia-bg.com
View	25	200.29.134.141	undefined
View	21	209.143.242.118	undefined
View	21	209.143.242.119	undefined
View	18	211.22.172.122	h122-172.hinet.net
View	16	209.73.164.48	av-dev4.sv.av.com
View	15	205.142.199.15	fw1.chmcc.org
View	15	208.35.215.250	ltsfoc.logictier.com
View	15	212.57.28.2	undefined

1 2 3 4 5 6 7 8 9 10 20

file:///C:/~~Documents and Settings/gcooper/Desktop/svsdemo/servlet/viewsummariesv4.html~~

Fig. 29


SVS - Event Summary - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History Links AltaVista - Welcome CNN.com Customize Links
Address file:///C:/Documents%20and%20Settings/gcooper/Desktop/svsdemo/servlet/viewsummaries.html?dateRange=today&fromMM=12&fromDD=31&fromYY=2000&froml
Go
SECURIFY
Security Chain Verification Service
profile log out help
Dashboard • Summary
Print Version
Conformance
Violators
Targets
today
377
213
85
32
29
20
12
11
11
11
377
189
0
DestIp:
209.143.242.118
1 2 3 4 5 6 7 8 9 10 20 30 40 NEXT
My Computer
3001
3002
3003
3004
2206

Events Summary

server time:
12.21.00 15:13
PST

7,153 violations of 1,131,477 total events (1%)

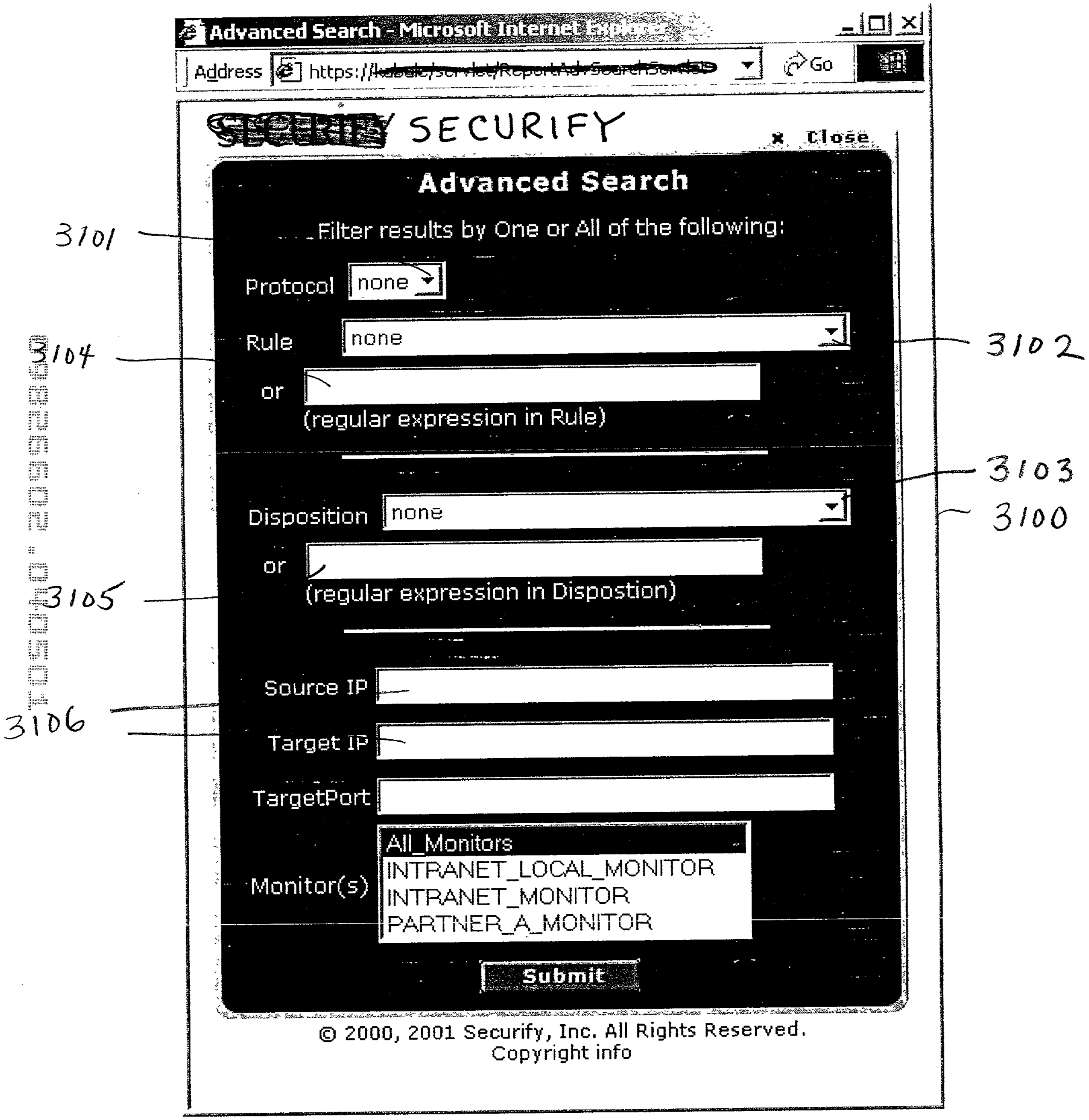
TARGETS

destination IP 12/19/2000-12/21/2000

Viewing: 1 - 15 of 1671

Detail	▾Count	IPDstAddress	TCP/UDPDstPort	DNSName
View	377	209.143.242.114	80	undefined
View	213	209.143.242.119	80	undefined
View	85	209.143.242.114	21	undefined
View	32	209.143.242.114	500	undefined
View	29	209.143.242.114	69	undefined
View	20	209.143.242.119	500	undefined
View	12	209.143.242.117	27374	undefined
View	11	209.143.242.114	27374	undefined
View	11	209.143.242.115	27374	undefined
View	11	209.143.242.118	27374	undefined
View	11	209.143.242.119	27374	undefined
View	11	209.143.242.121	27374	undefined
View	10	206.251.8.20	53	dns2.snv.gbix.net
View	10	209.251.8.84	25	dtmf.org
View	9	209.143.242.122	27374	undefined

Fig. 30



Advanced Search - Microsoft Internet Explorer

Address https://[redacted]

[redacted] SECURIFY

Advanced Search

Filter results by One or All of the following:

Protocol: none

Rule: none

or (regular expression in Rule)

Disposition: none

or (regular expression in Dispostion)

Source IP

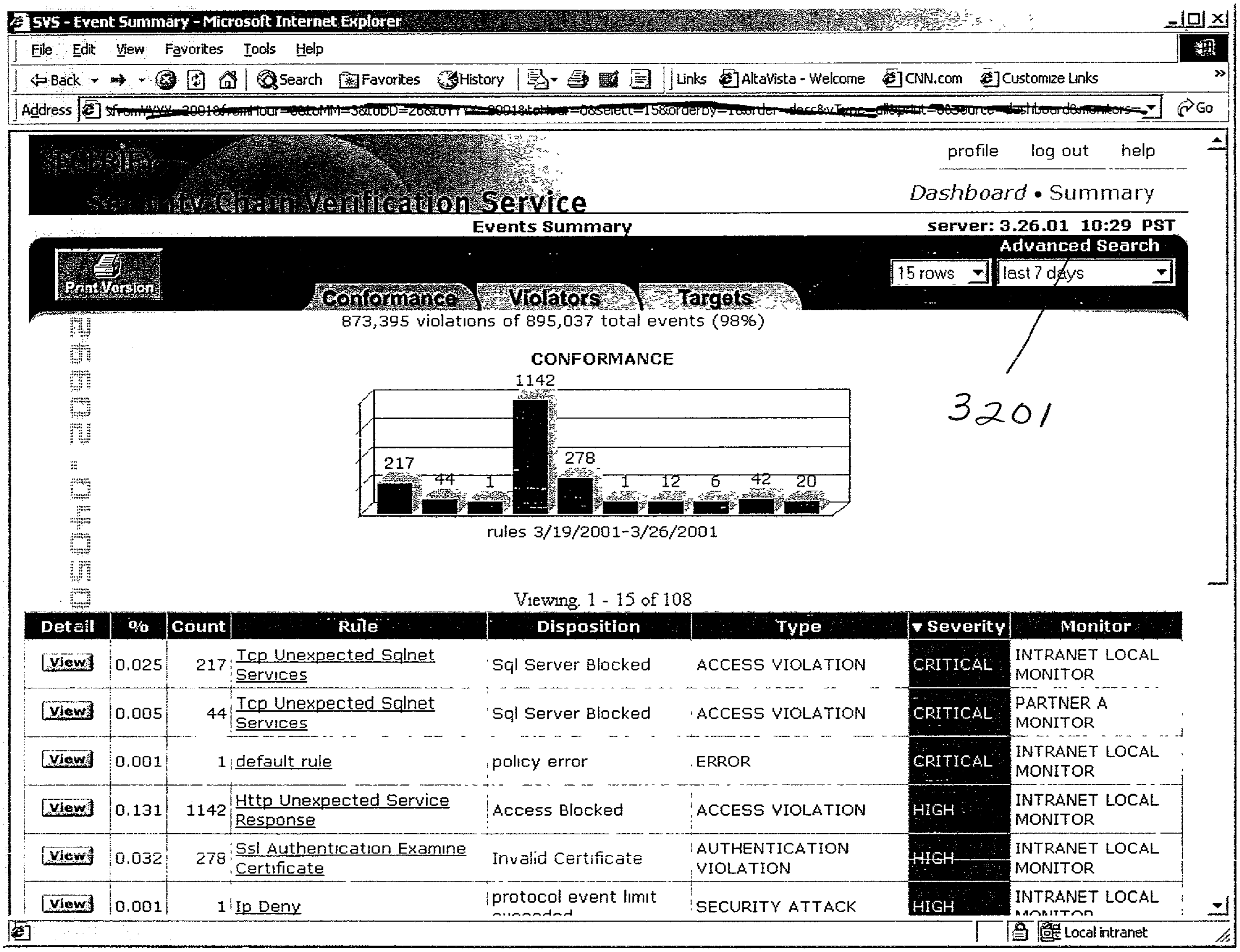
Target IP

TargetPort

Monitor(s):
All_Monitors
INTRANET_LOCAL_MONITOR
INTRANET_MONITOR
PARTNER_A_MONITOR

Submit

Fig. 31


SVS - Event Summary - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Links AltaVista - Welcome CNN.com Customize Links
Address [redacted]
Go
profile log out help
Dashboard • Summary
Security Chain Verification Service
Print Version
Advanced Search
15 rows
last 7 days
Conformance
Violators
Targets
3201
CONFORMANCE
217
44
1
1142
278
1
12
6
42
20
Local intranet

Events Summary

server: 3.26.01 10:29 PST

873,395 violations of 895,037 total events (98%)

rules 3/19/2001-3/26/2001

Viewing 1 - 15 of 108

Detail	%	Count	Rule	Disposition	Type	▾ Severity	Monitor
View	0.025	217	Tcp Unexpected Sqlnet Services	Sql Server Blocked	ACCESS VIOLATION	CRITICAL	INTRANET LOCAL MONITOR
View	0.005	44	Tcp Unexpected Sqlnet Services	Sql Server Blocked	ACCESS VIOLATION	CRITICAL	PARTNER A MONITOR
View	0.001	1	default rule	policy error	ERROR	CRITICAL	INTRANET LOCAL MONITOR
View	0.131	1142	Http Unexpected Service Response	Access Blocked	ACCESS VIOLATION	HIGH	INTRANET LOCAL MONITOR
View	0.032	278	Ssl Authentication Examine Certificate	Invalid Certificate	AUTHENTICATION VIOLATION	HIGH	INTRANET LOCAL MONITOR
View	0.001	1	Ip Deny	protocol event limit exceeded	SECURITY ATTACK	HIGH	INTRANET LOCAL MONITOR

Fig. 32